National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 - 31 May 2023 Vol. 10 No. 10

Table of Content

Vendor	Product	Page Number
hanwhavision	pnm-9084rqz1	1939
	pnm-9085rqz	1939
	pnm-9085rqz1	1940
	pnm-9322vqp	1941
	pnm-c12083rvd	1941
	pnm-c7083rvd	1942
	pnm-c9022rv	1943
	qnd-6010r	1943
	qnd-6011	1944
	qnd-6012r	1945
	qnd-6012r1	1945
	qnd-6020r	1946
	qnd-6021	1946
	qnd-6022r	1947
	qnd-6030r	1948
	qnd-6032r	1948
	qnd-6070r	1949
	qnd-6082r	1950
	qnd-6082r1	1950
	qnd-7010r	1951
	qnd-70142r	1951
	qnd-7020r	1952
	qnd-7022r	1953
	qnd-7030r	1953
	qnd-7032r	1954
	qnd-7080r	1955
	qnd-7082r	1955
	qnd-8010r	1956
	qnd-8011	1957
	qnd-8020r	1957
	qnd-8021	1958
	qnd-8030r	1958

Vendor	Product	Page Number
hanwhavision	qnd-8080r	1959
	qne-7080rvw	1960
	qne-7088rv	1960
	qne-8011r	1961
	qne-8021r	1962
	qnf-8010	1962
	qnf-9010	1963
	qno-6010r	1964
	qno-6012r	1964
	qno-6012r1	1965
	qno-6020r	1965
	qno-6022r	1966
	qno-6022r1	1967
	qno-6030r	1967
	qno-6032r	1968
	qno-6070r	1969
	qno-6082r	1969
	qno-6082r1	1970
	qno-7012r	1971
	qno-7020r	1971
	qno-7022r	1972
	qno-7030r	1972
	qno-7032r	1973
	qno-7080r	1974
	qno-7082r	1974
	qno-8010r	1975
	qno-8020r	1976
	qno-8030r	1976
	qno-8080r	1977
	qnp-6230	1978
	qnp-6230h	1978
	qnp-6230rh	1979

Vendor	Product	Page Number
IBM	power_system_e1080	2000
	power_system_e950	2001
	power_system_e980	2001
	power_system_h922	2002
	power_system_h924	2003
	power_system_l1022	2003
	power_system_l1024	2004
	power_system_l922	2005
	power_system_s1014	2006
	power_system_s1022	2006
	power_system_s1022s	2007
	power_system_s1024	2008
	power_system_s914	2008
	power_system_s922	2009
	power_system_s924	2010
icom	sr-7100vn	2011
	sr-7100vn\#31	2011
inaba	ac-wapu-300	2012
	ac-wapu-300-p	2012
	ac-wapum-300	2013
	ac-wapum-300-p	2013
jins	jins_meme	2014
Linksys	e2000	2014
	wrt54gl	2015
Mitsubishielectric	melsec_ws0-geth00200	2016
nissan	sylphy_classic_2021	2017
qrio	q-sl2	2017
Snapone	an-110-rt-2l1w	2018
	an-110-rt-2l1w-wifi	2023
	an-310-rt-4l2w	2027
	ovrc-300-pro	2032
	pakedge_rk-1	2040

Vendor	Product	Page Number
Cisco	business_350-16t-e-2g_firmware	2288
	business_350-16xts_firmware	2294
	business_350-24fp-4g_firmware	2301
	business_350-24fp-4x_firmware	2308
	business_350-24mgp-4x_firmware	2314
	business_350-24ngp-4x_firmware	2321
	business_350-24p-4g_firmware	2327
	business_350-24p-4x_firmware	2334
	business_350-24s-4g_firmware	2340
	business_350-24t-4g_firmware	2347
	business_350-24t-4x_firmware	2353
	business_350-24xs_firmware	2360
	business_350-24xts_firmware	2367
	business_350-24xt_firmware	2373
	business_350-48fp-4g_firmware	2380
	business_350-48fp-4x_firmware	2386
	business_350-48ngp-4x_firmware	2393
	business_350-48p-4g_firmware	2399
	business_350-48p-4x_firmware	2406
	business_350-48t-4g_firmware	2412
	business_350-48t-4x_firmware	2419
	business_350-48xt-4x_firmware	2426
	business_350-8fp-2g_firmware	2432
	business_350-8fp-e-2g_firmware	2439
	business_350-8mgp-2x_firmware	2445
	business_350-8mp-2x_firmware	2452
	business_350-8p-2g_firmware	2458
	business_350-8p-e-2g_firmware	2465
	business_350-8s-e-2g_firmware	2471
	business_350-8t-e-2g_firmware	2478
	business_350-8xt_firmware	2485
	sf200-24fp_firmware	2491

Vendor	Product	Page Number
Cisco	sf200-24p_firmware	2498
	sf200-24_firmware	2504
	sf200-48p_firmware	2511
	sf200-48_firmware	2517
	sf200e-24p_firmware	2524
	sf200e-24_firmware	2530
	sf200e-48p_firmware	2537
	sf200e-48_firmware	2544
	sf200e48p_firmware	2550
	sf250-08hp_firmware	2557
	sf250-08_firmware	2563
	sf250-10p_firmware	2570
	sf250-18_firmware	2576
	sf250-24p_firmware	2583
	sf250-24_firmware	2589
	sf250-26hp_firmware	2596
	sf250-26p_firmware	2603
	sf250-26_firmware	2609
	sf250-48hp_firmware	2616
	sf250-48_firmware	2622
	sf250-50hp_firmware	2629
	sf250-50p_firmware	2635
	sf250-50_firmware	2642
	sf250x-24p_firmware	2648
	sf250x-24_firmware	2655
	sf250x-48p_firmware	2662
	sf250x-48_firmware	2668
	sf300-08_firmware	2675
	sf300-24mp_firmware	2681
	sf300-24pp_firmware	2688
	sf300-24p_firmware	2694
	sf300-24_firmware	2701

Vendor	Product	Page Number
Cisco	sf300-48pp_firmware	2707
	sf300-48p_firmware	2714
	sf300-48_firmware	2721
	sf302-08mpp_firmware	2727
	sf302-08pp_firmware	2734
	sf302-08_firmware	2740
	sf350-08_firmware	2747
	sf350-10mp_firmware	2753
	sf350-10p_firmware	2760
	sf350-10sfp_firmware	2766
	sf350-10_firmware	2773
	sf350-20_firmware	2780
	sf350-24mp_firmware	2786
	sf350-24p_firmware	2793
	sf350-24_firmware	2799
	sf350-28mp_firmware	2806
	sf350-28p_firmware	2812
	sf350-28sfp_firmware	2819
	sf350-28_firmware	2825
	sf350-48mp_firmware	2832
	sf350-48p_firmware	2839
	sf350-48_firmware	2845
	sf350-52mp_firmware	2852
	sf350-52p_firmware	2858
	sf350-52_firmware	2865
	sf350-8mp_firmware	2871
	sf350-8pd_firmware	2878
	sf352-08mp_firmware	2884
	sf352-08p_firmware	2891
	sf352-08_firmware	2898
	sf355-10p_firmware	2904
	sf500-18p_firmware	2911

Vendor	Product	Page Number
Cisco	sf500-24mp_firmware	2917
	sf500-24p_firmware	2924
	sf500-24_firmware	2930
	sf500-48mp_firmware	2937
	sf500-48p_firmware	2943
	sf500-48_firmware	2950
	sf550x-24mp_firmware	2957
	sf550x-24p_firmware	2963
	sf550x-24_firmware	2970
	sf550x-48mp_firmware	2976
	sf550x-48p_firmware	2983
	sf550x-48_firmware	2989
	sg200-08p_firmware	2996
	sg200-08_firmware	3002
	sg200-10fp_firmware	3009
	sg200-18_firmware	3016
	sg200-26fp_firmware	3022
	sg200-26p_firmware	3029
	sg200-26_firmware	3035
	sg200-50fp_firmware	3042
	sg200-50p_firmware	3048
	sg200-50_firmware	3055
	sg250-08hp_firmware	3061
	sg250-08_firmware	3068
	sg250-10p_firmware	3075
	sg250-18_firmware	3081
	sg250-24p_firmware	3088
	sg250-24_firmware	3094
	sg250-26hp_firmware	3101
	sg250-26p_firmware	3107
	sg250-26_firmware	3114
	sg250-48hp_firmware	3120

Vendor	Product	Page Number
Cisco	sg250-48_firmware	3127
	sg250-50hp_firmware	3134
	sg250-50p_firmware	3140
	sg250-50_firmware	3147
	sg250x-24p_firmware	3153
	sg250x-24_firmware	3160
	sg250x-48p_firmware	3166
	sg250x-48_firmware	3173
	sg300-10mpp_firmware	3179
	sg300-10mp_firmware	3186
	sg300-10pp_firmware	3193
	sg300-10p_firmware	3199
	sg300-10sfp_firmware	3206
	sg300-10_firmware	3212
	sg300-20_firmware	3219
	sg300-28mp_firmware	3225
	sg300-28pp_firmware	3232
	sg300-28p_firmware	3238
	sg300-28sfp_firmware	3245
	sg300-28_firmware	3252
	sg300-52mp_firmware	3258
	sg300-52p_firmware	3265
	sg300-52_firmware	3271
	sg350-10mp_firmware	3278
	sg350-10p_firmware	3284
	sg350-10_firmware	3291
	sg350-28mp_firmware	3297
	sg350-28p_firmware	3304
	sg350-28_firmware	3311
	sg350x-12pmv_firmware	3317
	sg350x-24mp_firmware	3324
	sg350x-24pd_firmware	3330

Vendor	Product	Page Number
Cisco	sg350x-24pv_firmware	3337
	sg350x-24p_firmware	3343
	sg350x-24_firmware	3350
	sg350x-48mp_firmware	3356
	sg350x-48pv_firmware	3363
	sg350x-48p_firmware	3370
	sg350x-48_firmware	3376
	sg350x-8pmd_firmware	3383
	sg350xg-24f_firmware	3389
	sg350xg-24t_firmware	3396
	sg350xg-2f10_firmware	3402
	sg350xg-48t_firmware	3409
	sg355-10mp_firmware	3415
	sg355-10p_firmware	3422
	sg500-28mpp_firmware	3429
	sg500-28pp_firmware	3435
	sg500-28p_firmware	3442
	sg500-28_firmware	3448
	sg500-52pp_firmware	3455
	sg500-52p_firmware	3461
	sg500x-24mpp_firmware	3468
	sg500x-24p_firmware	3474
	sg500x-24_firmware	3481
	sg500x-48mpp_firmware	3488
	sg500x-48mp_firmware	3494
	sg500x-48p_firmware	3501
	sg500x-48_firmware	3507
	sg500x24mpp_firmware	3514
	sg500xg-8f8t_firmware	3520
	sg500xg8f8t_firmware	3527
	sg550x-24mpp_firmware	3533
	sg550x-24mp_firmware	3540

Vendor	Product	Page Number
Cisco	sg550x-24p_firmware	3547
	sg550x-24_firmware	3553
	sg550x-48mp_firmware	3560
	sg550x-48p_firmware	3566
	sg550x-48t_firmware	3573
	sg550x-48_firmware	3579
	sg550xg-24f_firmware	3586
	sg550xg-24t_firmware	3533
	sg550xg-48t_firmware	3599
	sg550xg-8f8t_firmware	3606
contec	solarview_compact_firmware	3612
	sv-cpt-mc310f_firmware	3612
	sv-cpt-mc310_firmware	3615
Debian	debian_linux	3618
Dell	dss_8440_firmware	3623
	emc_storage_nx3240_firmware	3623
	emc_storage_nx3340_firmware	3624
	emc_xc_core_6420_firmware	3625
	emc_xc_core_xc640_firmware	3626
	emc_xc_core_xc740xd2_firmware	3626
	emc_xc_core_xc740xd_firmware	3627
	emc_xc_core_xc940_firmware	3628
	emc_xc_core_xcxr2_firmware	3629
	poweredge_c4140_firmware	3629
	poweredge_c6420_firmware	3630
	poweredge_fc640_firmware	3631
	poweredge_m640_firmware	3631
	poweredge_mx740c_firmware	3632
	poweredge_mx840c_firmware	3633
	poweredge_r440_firmware	3634
	poweredge_r540_firmware	3634
	poweredge_r640_firmware	3635

Vendor	Product	Page Number
hanwhavision	anv-l6082r_firmware	3677
	anv-l7012r_firmware	3677
	anv-l7082r_firmware	3678
	pnm-12082rvd_firmware	3678
	pnm-7002vd_firmware	3679
	pnm-7082rvd_firmware	3680
	pnm-8082vt_firmware	3680
	pnm-9000qb_firmware	3681
	pnm-9000vd_firmware	3682
	pnm-9002vq_firmware	3682
	pnm-9022v_firmware	3683
	pnm-9031rv_firmware	3684
	pnm-9084qz1_firmware	3684
	pnm-9084rqz1_firmware	3685
	pnm-9084rqz_firmware	3685
	pnm-9085rqz1_firmware	3686
	pnm-9085rqz_firmware	3687
	pnm-9322vqp_firmware	3687
	pnm-c12083rvd_firmware	3688
	pnm-c7083rvd_firmware	3689
	pnm-c9022rv_firmware	3689
	qnd-6010r_firmware	3690
	qnd-6011_firmware	3691
	qnd-6012r1_firmware	3691
	qnd-6012r_firmware	3692
	qnd-6020r_firmware	3692
	qnd-6021_firmware	3693
	qnd-6022r_firmware	3694
	qnd-6030r_firmware	3694
	qnd-6032r_firmware	3695
	qnd-6070r_firmware	3696
	qnd-6082r1_firmware	3696

Vendor	Product	Page Number
hanwhavision	qnd-6082r_firmware	3697
	qnd-7010r_firmware	3698
	qnd-70142r_firmware	3698
	qnd-7020r_firmware	3699
	qnd-7022r_firmware	3699
	qnd-7030r_firmware	3700
	qnd-7032r_firmware	3701
	qnd-7080r_firmware	3701
	qnd-7082r_firmware	3702
	qnd-8010r_firmware	3703
	qnd-8011_firmware	3703
	qnd-8020r_firmware	3704
	qnd-8021_firmware	3705
	qnd-8030r_firmware	3705
	qnd-8080r_firmware	3706
	qne-7080rvw_firmware	3706
	qne-7088rv_firmware	3707
	qne-8011r_firmware	3708
	qne-8021r_firmware	3708
	qnf-8010_firmware	3709
	qnf-9010_firmware	3710
	qno-6010r_firmware	3710
	qno-6012r1_firmware	3711
	qno-6012r_firmware	3712
	qno-6020r_firmware	3712
	qno-6022r1_firmware	3713
	qno-6022r_firmware	3713
	qno-6030r_firmware	3714
	qno-6032r_firmware	3715
	qno-6070r_firmware	3715
	qno-6082r1_firmware	3716
	qno-6082r_firmware	3717

Vendor	Product	Page Number
hanwhavision	qno-7012r_firmware	3717
	qno-7020r_firmware	3718
	qno-7022r_firmware	3719
	qno-7030r_firmware	3719
	qno-7032r_firmware	3720
	qno-7080r_firmware	3720
	qno-7082r_firmware	3721
	qno-8010r_firmware	3722
	qno-8020r_firmware	3722
	qno-8030r_firmware	3723
	qno-8080r_firmware	3724
	qnp-6230h_firmware	3724
	qnp-6230rh_firmware	3725
	qnp-6230_firmware	3726
	qnp-6250h_firmware	3726
	qnp-6250r_firmware	3727
	qnp-6250_firmware	3727
	qnp-6320hs_firmware	3728
	qnp-6320h_firmware	3729
	qnp-6320r_firmware	3729
	qnp-6320_firmware	3730
	qnv-6010r_firmware	3731
	qnv-6012r1_firmware	3731
	qnv-6012r_firmware	3732
	qnv-6020r_firmware	3733
	qnv-6022r1_firmware	3733
	qnv-6022r_firmware	3734
	qnv-6030r_firmware	3734
	qnv-6032r_firmware	3735
	qnv-6070r_firmware	3736
	qnv-6082r1_firmware	3736
	qnv-6082r_firmware	3737

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 0kims					
Product: snarkjs					
Affected Version(s): * Up to (including) 0.6.11					
N/A	21-May-2023	7.5	iden3 snarkjs through 0.6.11 allows double spending because there is no validation that the publicSignals length is less than the field modulus. **CVE ID : CVE-2023-33252**	N/A	A-0KI-SNAR-020623/1
Vendor: 3DS					
Product: 3dexperience					
Affected Version(s): From (including) r2018x Up to (including) r2023x					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-2023	6.1	A reflected Cross-site Scripting (XSS) vulnerability in 3DEXPERIENCE R2018x through R2023x allows an attacker to execute arbitrary script code. **CVE ID : CVE-2023-1996**	https://www.3ds.com/vulnerability/advisories	A-3DS-3DEX-020623/2
Vendor: about_me_3000_widget_project					
Product: about_me_3000_widget					
Affected Version(s): * Up to (including) 2.2.6					
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Csaba Kissi About Me 3000 widget	N/A	A-ABO-ABOU-020623/3

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin <= 2.2.6 versions. **CVE ID : CVE-2023-25474**		
Vendor: Acronis					
Product: cyber_infrastructure					
Affected Version(s): * Up to (excluding) 5.3.1-38					
Incorrect Authorization	18-May-2023	5.5	Sensitive information disclosure due to improper authorization. The following products are affected: Acronis Cyber Infrastructure (ACI) before build 5.3.1-38. **CVE ID : CVE-2023-2782**	https://security-advisory.acronis.com/advisories/SEC-3475	A-ACR-CYBE-020623/4
Vendor: adampos					
Product: mobilmen_el_terminali_yazilimi					
Affected Version(s): * Up to (excluding) 3					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-May-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Adam Retail Automation Systems Mobilmen Terminal Software allows SQL Injection.This issue affects Mobilmen Terminal Software: before 3.	N/A	A-ADA-MOBI-020623/5

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1508		
Vendor: admin_block_country_project					
Product: admin_block_country					
Affected Version(s): * Up to (including) 7.1.4					
Cross-Site Request Forgery (CSRF)	26-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in TheOnlineHero - Tom Skroza Admin Block Country plugin <= 7.1.4 versions. **CVE ID : CVE-2023-24007**	N/A	A-ADM-ADMI-020623/6
Vendor: alist_project					
Product: alist					
Affected Version(s): 3.15.1					
N/A	23-May-2023	7.5	AList 3.15.1 is vulnerable to Incorrect Access Control, which can be exploited by attackers to obtain sensitive information. **CVE ID : CVE-2023-31726**	N/A	A-ALI-ALIS-020623/7
Vendor: Alkacon					
Product: opencms					
Affected Version(s): 11.0					
Improper Neutralization of Input During Web Page Generation	16-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in alkacon-OpenCMS v11.0.0.0 allows attackers to execute arbitrary web	https://github.com/alkacon/opencms-core/commit/21bfbeaf6b038e2c03bb421	A-ALK-OPEN-020623/8

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			scripts or HTML via a crafted payload injected into the Title field under the Upload Image module. **CVE ID : CVE-2023-31544**	ce7f0933dd7a7633e	
Vendor: allwaysync					
Product: allwaysync					
Affected Version(s): 19.0.3.0					
Incorrect Default Permissions	22-May-2023	7.8	Insecure Permission vulnerability found in Botkind/Siber Systems SyncApp v.19.0.3.0 allows a local attacker toe escalate privileges via the SyncService.exe file. **CVE ID : CVE-2023-29838**	N/A	A-ALL-ALLW-020623/9
Vendor: Apache					
Product: inlong					
Affected Version(s): 1.5.0					
Insecure Default Initialization of Resource	22-May-2023	6.5	Insecure Default Initialization of Resource Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.5.0 through 1.6.0. Users registered in InLong who joined later can see deleted users' data. Users are advised	https://lists.apache.org/thread/shvwwr6toqz5rr39rwh4k03z08sh9jmr	A-APA-INLO-020623/10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7836 https://github.com/apache/inlong/pull/7836 to solve it. **CVE ID : CVE-2023-31101**		
Affected Version(s): 1.6.0					
Insecure Default Initialization of Resource	22-May-2023	6.5	Insecure Default Initialization of Resource Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.5.0 through 1.6.0. Users registered in InLong who joined later can see deleted users' data. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7836 https://github.com/apache/inlong/pull/7836 to solve it.	https://lists.apache.org/thread/shvwwr6toqz5rr39rwh4k03z08sh9jmr	A-APA-INLO-020623/11

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31101		
Affected Version(s): From (including) 1.1.0 Up to (including) 1.6.0					
Weak Password Requirements	22-May-2023	9.8	Weak Password Requirements vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.1.0 through 1.6.0. When users change their password to a simple password (with any character or symbol), attackers can easily guess the user's password and access the account. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7805 https://github.com/apache/inlong/pull/7805 to solve it. **CVE ID : CVE-2023-31098**	https://lists.apache.org/thread/1fvloc3no1gbffzrcsx9ltsg08wr2d1w	A-APA-INLO-020623/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 1.2.0 Up to (including) 1.6.0					
Improper Privilege Management	22-May-2023	9.8	Improper Privilege Management Vulnerabilities in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0. When the attacker has access to a valid (but unprivileged) account, the exploit can be executed using Burp Suite by sending a login request and following it with a subsequent HTTP request using the returned cookie. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7836 https://github.com/apache/inlong/pull/7836 to solve it.	https://lists.apache.org/thread/btorjbo9o71h22tcvxzy076022hjdzq0	A-APA-INLO-020623/13

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31062		
Files or Directories Accessible to External Parties	22-May-2023	7.5	Files or Directories Accessible to External Parties vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0. the user in InLong could cancel an application that doesn't belongs to it. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7799 https://github.com/apache/inlong/pull/7799 to solve it. **CVE ID : CVE-2023-31064**	https://lists.apache.org/thread/1osd2k3t3qol2wdsswqtr9gxdkf78n00	A-APA-INLO-020623/14
Incorrect Permission Assignment for Critical Resource	22-May-2023	7.5	Incorrect Permission Assignment for Critical Resource Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0.	https://lists.apache.org/thread/9nz8o2skgc5230w276h4w92j0zstnl06	A-APA-INLO-020623/15

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The attacker can delete others' subscriptions, even if they are not the owner of the deleted subscription. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick [1] to solve it. [1] https://github.com/apache/inlong/pull/7949 https://github.com/apache/inlong/pull/7949 **CVE ID : CVE-2023-31453**		
Incorrect Permission Assignment for Critical Resource	22-May-2023	7.5	Incorrect Permission Assignment for Critical Resource Vulnerability in Apache Software Foundation Apache	https://lists.apache.org/thread/nqt1tr6pbq8q4b033d7sg5gltx5pmjgl	A-APA-INLO-020623/16

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0. The attacker can bind any cluster, even if he is not the cluster owner. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick [1] to solve it.[1] https://github.com/apache/inlong/pull/7947 https://github.com/apache/inlong/pull/7947 **CVE ID : CVE-2023-31454**		
Affected Version(s): From (including) 1.4.0 Up to (including) 1.6.0					
Insufficient Session Expiration	22-May-2023	9.1	Insufficient Session Expiration vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0.	https://lists.apache.org/thread/to7o0n2cks0omtwo6mhh5cs2vfdbplqf	A-APA-INLO-020623/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			An old session can be used by an attacker even after the user has been deleted or the password has been changed. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7836 https://github.com/apache/inlong/pull/7836 , https://github.com/apache/inlong/pull/7884 https://github.com/apache/inlong/pull/7884 to solve it. **CVE ID : CVE-2023-31065**		
Files or Directories Accessible to External Parties	22-May-2023	9.1	Files or Directories Accessible to External Parties vulnerability in Apache Software Foundation Apache InLong.This issue	https://lists.apache.org/thread/x7y05wo37sq5l9fnmmsjh2dr9kcjrcxf	A-APA-INLO-020623/18

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affects Apache InLong: from 1.4.0 through 1.6.0. Different users in InLong could delete, edit, stop, and start others' sources! Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7775 https://github.com/apache/inlong/pull/7775 to solve it. **CVE ID : CVE-2023-31066**		
Deserialization of Untrusted Data	22-May-2023	7.5	Deserialization of Untrusted Data Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. Attackers would bypass the 'autoDeserialize' option filtering by adding blanks. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick	https://lists.apache.org/thread/bkcgbn9l61croxfyspf7xd42qb189s3z	A-APA-INLO-020623/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			https://github.com/apache/inlong/pull/7674 https://github.com/apache/inlong/pull/7674 to solve it. **CVE ID : CVE-2023-31058**		
Exposure of Resource to Wrong Sphere	22-May-2023	7.5	Exposure of Resource to Wrong Sphere Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. Attackers can change the immutable name and type of cluster of InLong. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7891 https://github.com/apache/inlong/pull/7891 to solve it.	https://lists.apache.org/thread/bv51zhjookcnfbz8b0xsl9wv78sn0j1p	A-APA-INLO-020623/20

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31103		
Exposure of Resource to Wrong Sphere	22-May-2023	7.5	Exposure of Resource to Wrong Sphere Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. Attackers can change the immutable name and type of nodes of InLong. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick [1] to solve it. [1] https://cveprocess.apache.org/cve5/[1]%C2%A0https://github.com/apache/inlong/pull/7891 https://github.com/apache/inlong/pull/7891 https://github.com/apache/inlong/pull/7891 **CVE ID : CVE-2023-31206**	https://lists.apache.org/thread/qb7zffo785wzpmsobjqcypodngw6kg6x	A-APA-INLO-020623/21
Product: rocketmq					
Affected Version(s): * Up to (excluding) 5.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	24-May-2023	9.8	For RocketMQ versions 5.1.0 and below, under certain conditions, there is a risk of remote command execution. Several components of RocketMQ, including NameServer, Broker, and Controller, are leaked on the extranet and lack permission verification, an attacker can exploit this vulnerability by using the update configuration function to execute commands as the system users that RocketMQ is running as. Additionally, an attacker can achieve the same effect by forging the RocketMQ protocol content. To prevent these attacks, users are recommended to upgrade to version 5.1.1 or above for using RocketMQ 5.x or 4.9.6 or	https://lists.apache.org/thread/1s8j2c8kogthtpv3060yddk03zq0pxyp	A-APA-ROCK-020623/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			above for using RocketMQ 4.x . **CVE ID : CVE-2023-33246**		
Product: tomcat					
Affected Version(s): 11.0.0					
Off-by-one Error	22-May-2023	7.5	The fix for CVE-2023-24998 was incomplete for Apache Tomcat 11.0.0-M2 to 11.0.0-M4, 10.1.5 to 10.1.7, 9.0.71 to 9.0.73 and 8.5.85 to 8.5.87. If non-default HTTP connector settings were used such that the maxParameterCount could be reached using query string parameters and a request was submitted that supplied exactly maxParameterCoun	https://lists.apache.org/thread/7wvxonzwb7k9hx9jt3q33cmy7j97jo3j	A-APA-TOMC-020623/23

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			t parameters in the query string, the limit for uploaded request parts could be bypassed with the potential for a denial of service to occur. **CVE ID : CVE-2023-28709**		
Affected Version(s): From (including) 10.1.5 Up to (including) 10.1.7					
Off-by-one Error	22-May-2023	7.5	The fix for CVE-2023-24998 was incomplete for Apache Tomcat 11.0.0-M2 to 11.0.0-M4, 10.1.5 to 10.1.7, 9.0.71 to 9.0.73 and 8.5.85 to 8.5.87. If non-default HTTP connector settings were used such that the maxParameterCount could be reached using query string parameters and a request was submitted that supplied exactly maxParameterCount parameters in the query string, the limit for uploaded request parts could	https://lists.apache.org/thread/7wvxonzwb7k9hx9jt3q33cmy7j97jo3j	A-APA-TOMC-020623/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be bypassed with the potential for a denial of service to occur. **CVE ID : CVE-2023-28709**		
Affected Version(s): From (including) 8.5.85 Up to (including) 8.5.87					
Off-by-one Error	22-May-2023	7.5	The fix for CVE-2023-24998 was incomplete for Apache Tomcat 11.0.0-M2 to 11.0.0-M4, 10.1.5 to 10.1.7, 9.0.71 to 9.0.73 and 8.5.85 to 8.5.87. If non-default HTTP connector settings were used such that the maxParameterCount could be reached using query string parameters and a request was submitted that supplied exactly maxParameterCount parameters in the query string, the limit for uploaded request parts could be bypassed with the potential for a denial of service to occur.	https://lists.apache.org/thread/7wvxonzwb7k9hx9jt3q33cmy7j97jo3j	A-APA-TOMC-020623/25

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28709		
Affected Version(s): From (including) 9.0.71 Up to (including) 9.0.73					
Off-by-one Error	22-May-2023	7.5	The fix for CVE-2023-24998 was incomplete for Apache Tomcat 11.0.0-M2 to 11.0.0-M4, 10.1.5 to 10.1.7, 9.0.71 to 9.0.73 and 8.5.85 to 8.5.87. If non-default HTTP connector settings were used such that the maxParameterCount could be reached using query string parameters and a request was submitted that supplied exactly maxParameterCount parameters in the query string, the limit for uploaded request parts could be bypassed with the potential for a denial of service to occur.	https://lists.apache.org/thread/7wvxonzwb7k9hx9jt3q33cmy7j97jo3j	A-APA-TOMC-020623/26

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28709		
Vendor: archivist_project					
Product: archivist					
Affected Version(s): * Up to (including) 1.7.4					
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Eric Teubert Archivist – Custom Archive Templates plugin <= 1.7.4 versions. **CVE ID : CVE-2023-25448**	N/A	A-ARC-ARCH-020623/27
Vendor: Artistscope					
Product: copysafe_web_protection					
Affected Version(s): * Up to (excluding) 3.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ArtistScope CopySafe Web Protection plugin <= 3.13 versions. **CVE ID : CVE-2023-29098**	N/A	A-ART-COPY-020623/28
Vendor: Arubanetworks					
Product: edgeconnect_enterprise					
Affected Version(s): * Up to (including) 9.0.8.0					
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30501**		
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30502**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/30

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise comman d line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitat ion of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operatin g system leading to complete system compromise. **CVE ID : CVE-2023-30503**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/31
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise comman d line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitat ion of these vulnerabilities result in the ability to execute arbitrary commands as root	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30504**		
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30505**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/33
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30506**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-May-2023	6.5	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-30507**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/35
Improper Limitation of a Pathname to a Restricted Directory	16-May-2023	6.5	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/36

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-30508**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-May-2023	6.5	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-30509**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/37
N/A	16-May-2023	4.3	A vulnerability exists in the Aruba EdgeConnect Enterprise web management interface that allows remote authenticated users to issue arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/38

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			URL requests from the Aruba EdgeConnect Enterprise instance. The impact of this vulnerability is limited to a subset of URLs which can result in the possible disclosure of data due to the network position of the Aruba EdgeConnect Enterprise instance. **CVE ID : CVE-2023-30510**		
Affected Version(s): From (including) 9.1.0.0 Up to (including) 9.1.5.0					
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30501		
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30502**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/40
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30503**		
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30504**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/42
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/43

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30505**		
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30506**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-May-2023	6.5	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-30507**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/45
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-May-2023	6.5	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-30508**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-May-2023	6.5	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-30509**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/47
N/A	16-May-2023	4.3	A vulnerability exists in the Aruba EdgeConnect Enterprise web management interface that allows remote authenticated users to issue arbitrary URL requests from the Aruba EdgeConnect Enterprise instance. The impact of this vulnerability is limited to a subset of URLs which can result in the possible disclosure of data due to the network position of the Aruba	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/48

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			EdgeConnect Enterprise instance. **CVE ID : CVE-2023-30510**		
Affected Version(s): From (including) 9.2.0.0 Up to (including) 9.2.3.0					
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30501**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/49
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitat	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/50

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ion of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30502**		
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30503**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/51
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that	https://www.arubanetworks.com/assets/alert/ARUBA-	A-ARU-EDGE-020623/52

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise. **CVE ID : CVE-2023-30504**	PSA-2023-0007.txt	
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/53

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30505		
N/A	16-May-2023	8.8	Vulnerabilities exist in the Aruba EdgeConnect Enterprise comman d line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitat ion of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operatin g system leading to complete system compromise. **CVE ID : CVE-2023-30506**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/54
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-May-2023	6.5	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successfu l exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operatin	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/55

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			g system, including sensitive system files. **CVE ID : CVE-2023-30507**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-May-2023	6.5	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files. **CVE ID : CVE-2023-30508**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/56
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-May-2023	6.5	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/57

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive system files. **CVE ID : CVE-2023-30509**		
N/A	16-May-2023	4.3	A vulnerability exists in the Aruba EdgeConnect Enterprise web management interface that allows remote authenticated users to issue arbitrary URL requests from the Aruba EdgeConnect Enterprise instance. The impact of this vulnerability is limited to a subset of URLs which can result in the possible disclosure of data due to the network position of the Aruba EdgeConnect Enterprise instance. **CVE ID : CVE-2023-30510**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-0007.txt	A-ARU-EDGE-020623/58
Vendor: Asustor					
Product: adm					
Affected Version(s): 4.0.0					
Improper Neutralization of Input During Web Page Generation	17-May-2023	6.1	A Cross-Site Scripting(XSS) vulnerability was found on ADM, LooksGood and SoundsGood Apps. An attacker can exploit this vulnerability to	https://www.asustor.com/security/security_advisory_detail?id=22	A-ASU-ADM-020623/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			inject malicious scripts into the target applications to access any cookies or sensitive information retained by the browser and used with that application. Affected products and versions include: ADM 4.0.6.REG2, 4.1.0 and below as well as ADM 4.2.1.RGE2 and below, LooksGood 2.0.0.R129 and below and SoundsGood 2.3.0.r1027 and below. **CVE ID : CVE-2023-2509**		
Affected Version(s): 4.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	6.1	A Cross-Site Scripting(XSS) vulnerability was found on ADM, LooksGood and SoundsGood Apps. An attacker can exploit this vulnerability to inject malicious scripts into the target applications to access any cookies or sensitive information retained by the browser and used	https://www.asustor.com/security/security_advisory_detail?id=22	A-ASU-ADM-020623/60

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with that application. Affected products and versions include: ADM 4.0.6.REG2, 4.1.0 and below as well as ADM 4.2.1.RGE2 and below, LooksGood 2.0.0.R129 and below and SoundsGood 2.3.0.r1027 and below. **CVE ID : CVE-2023-2509**		
Affected Version(s): 4.1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	6.1	A Cross-Site Scripting(XSS) vulnerability was found on ADM, LooksGood and SoundsGood Apps. An attacker can exploit this vulnerability to inject malicious scripts into the target applications to access any cookies or sensitive information retained by the browser and used with that application. Affected products and versions include: ADM 4.0.6.REG2, 4.1.0 and below as well as ADM 4.2.1.RGE2	https://www.asustor.com/security/security_advisory_detail?id=22	A-ASU-ADM-020623/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and below, LooksGood 2.0.0.R129 and below and SoundsGood 2.3.0.r1027 and below. **CVE ID : CVE-2023-2509**		
Affected Version(s): 4.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	6.1	A Cross-Site Scripting(XSS) vulnerability was found on ADM, LooksGood and SoundsGood Apps. An attacker can exploit this vulnerability to inject malicious scripts into the target applications to access any cookies or sensitive information retained by the browser and used with that application. Affected products and versions include: ADM 4.0.6.REG2, 4.1.0 and below as well as ADM 4.2.1.RGE2 and below, LooksGood 2.0.0.R129 and below and SoundsGood 2.3.0.r1027 and below.	https://www.asustor.com/security/security_advisory_detail?id=22	A-ASU-ADM-020623/62

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2509		
Product: looksgood					
Affected Version(s): 2.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	6.1	A Cross-Site Scripting(XSS) vulnerability was found on ADM, LooksGood and SoundsGood Apps. An attacker can exploit this vulnerability to inject malicious scripts into the target applications to access any cookies or sensitive information retained by the browser and used with that application. Affected products and versions include: ADM 4.0.6.REG2, 4.1.0 and below as well as ADM 4.2.1.RGE2 and below, LooksGood 2.0.0.R129 and below and SoundsGood 2.3.0.r1027 and below. **CVE ID : CVE-2023-2509**	https://www.asustor.com/security/security_advisory_detail?id=22	A-ASU-LOOK-020623/63
Product: soundsgood					
Affected Version(s): 2.3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	6.1	A Cross-Site Scripting(XSS) vulnerability was found on ADM, LooksGood and SoundsGood Apps. An attacker can exploit this vulnerability to inject malicious scripts into the target applications to access any cookies or sensitive information retained by the browser and used with that application. Affected products and versions include: ADM 4.0.6.REG2, 4.1.0 and below as well as ADM 4.2.1.RGE2 and below, LooksGood 2.0.0.R129 and below and SoundsGood 2.3.0.r1027 and below. **CVE ID : CVE-2023-2509**	https://www.asustor.com/security/security_advisory_detail?id=22	A-ASU-SOUN-020623/64
Vendor: autoaffiliatelinks					
Product: auto_affiliate_links					
Affected Version(s): * Up to (including) 6.3					
Cross-Site Request Forgery (CSRF)	20-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Lucian Apostol Auto Affiliate Links	N/A	A-AUT-AUTO-020623/65

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin <= 6.3 versions. **CVE ID : CVE-2023-22689**		
Vendor: baidu_tongji_generator_project					
Product: baidu_tongji_generator					
Affected Version(s): * Up to (including) 1.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Haoqisir Baidu Tongji generator plugin <= 1.0.2 versions. **CVE ID : CVE-2023-31233**	N/A	A-BAI-BAID-020623/66
Vendor: beekeeperstudio					
Product: beekeeper-studio					
Affected Version(s): * Up to (excluding) 3.9.9					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	8.8	Beekeeper Studio versions prior to 3.9.9 allows a remote authenticated attacker to execute arbitrary JavaScript code with the privilege of the application on the PC where the affected product is installed. As a result, an arbitrary OS command may be executed as well. **CVE ID : CVE-2023-28394**	N/A	A-BEE-BEEK-020623/67
Vendor: berocket					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: brands_for_woocommerce					
Affected Version(s): * Up to (including) 3.7.0.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in BeRocket Brands for WooCommerce plugin <= 3.7.0.6 versions. **CVE ID : CVE-2023-23667**	N/A	A-BER-BRAN-020623/68
Vendor: Bitcoin					
Product: bitcoin_core					
Affected Version(s): * Up to (excluding) 24.1					
Uncontrolled Resource Consumption	22-May-2023	7.5	Bitcoin Core before 24.1, when debug mode is not used, allows attackers to cause a denial of service (CPU consumption) because draining the inventory-to-send queue is inefficient, as exploited in the wild in May 2023. **CVE ID : CVE-2023-33297**	https://github.com/bitcoin/bitcoin/pull/27610	A-BIT-BITC-020623/69
Vendor: bludit					
Product: bludit					
Affected Version(s): 4.0.0					
N/A	16-May-2023	8.8	An issue in Bludit 4.0.0-rc-2 allows authenticated attackers to change the Administrator password and	N/A	A-BLU-BLUD-020623/70

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalate privileges via a crafted request. **CVE ID : CVE-2023-31572**		
Affected Version(s): 3.14.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	5.4	Bludit v3.14.1 is vulnerable to Stored Cross Site Scripting (XSS) via SVG file on site logo. **CVE ID : CVE-2023-31698**	N/A	A-BLU-BLUD-020623/71
Vendor: Brother					
Product: iprint\&scan					
Affected Version(s): * Up to (excluding) 6.11.3					
N/A	18-May-2023	3.3	Brother iPrint&Scan V6.11.2 and earlier contains an improper access control vulnerability. This vulnerability may be exploited by the other app installed on the victim user's Android device, which may lead to displaying the settings and/or log information of the affected app as a print preview. **CVE ID : CVE-2023-28369**	https://faq.brother.co.jp/app/answers/detail/a_id/13468	A-BRO-IPRI-020623/72
Vendor: budget_and_expense_tracker_system_project					
Product: budget_and_expense_tracker_system					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-2023	8.8	A vulnerability, which was classified as critical, was found in SourceCodester Budget and Expense Tracker System 1.0. Affected is an unknown function of the file /admin/budget/manage_budget.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-229278 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-2772**	N/A	A-BUD-BUDG-020623/73
Vendor: bumsys_project					
Product: bumsys					
Affected Version(s): * Up to (excluding) 2.2.0					
Improper Neutralization of Special Elements used in an SQL	22-May-2023	7.2	SQL Injection in GitHub repository unilogies/bumsys prior to 2.2.0. **CVE ID : CVE-2023-2832**	https://huntr.dev/bounties/37b80402-0edf-4f26-a668-b6f8b48dcdfb, https://github	A-BUM-BUMS-020623/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')				.com/unilogies/bumsys/commit/1b426f58a513194206d0ea8ab58baf1461e54978	
Vendor: bus_dispatch_and_information_system_project					
Product: bus_dispatch_and_information_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-2023	9.8	A vulnerability was found in code-projects Bus Dispatch and Information System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file view_branch.php. The manipulation of the argument branchid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229280. **CVE ID : CVE-2023-2774**	N/A	A-BUS-BUS_-020623/75
Improper Neutralization of Special Elements used in an	28-May-2023	9.1	A vulnerability classified as critical has been found in code-projects Bus Dispatch and Information System	N/A	A-BUS-BUS_-020623/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			1.0. Affected is an unknown function of the file delete_bus.php. The manipulation of the argument busid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-230112. **CVE ID : CVE-2023-2951**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-2023	8.8	A vulnerability has been found in code-projects Bus Dispatch and Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file view_admin.php. The manipulation of the argument adminid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this	N/A	A-BUS-BUS_-020623/77

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-229279. **CVE ID : CVE-2023-2773**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-2023	8.8	A vulnerability was found in code-projects Bus Dispatch and Information System 1.0. It has been classified as critical. This affects an unknown part of the file adminHome.php. The manipulation of the argument reach_city leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-229281 was assigned to this vulnerability. **CVE ID : CVE-2023-2775**	N/A	A-BUS-BUS_-020623/78
Vendor: cbot					
Product: cbot_core					
Affected Version(s): * Up to (excluding) 4.0.3.4					
N/A	25-May-2023	9.8	Generation of Incorrect Security Tokens vulnerability in CBOT Chatbot allows Token Impersonation, Privilege	N/A	A-CBO-CBOT-020623/79

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Abuse.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7. **CVE ID : CVE-2023-2882**		
Use of Insufficiently Random Values	25-May-2023	9.8	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG), Use of Insufficiently Random Values vulnerability in CBOT Chatbot allows Signature Spoofing by Key Recreation.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7. **CVE ID : CVE-2023-2884**	N/A	A-CBO-CBOT-020623/80
Authorization Bypass Through User-Controlled Key	25-May-2023	8.8	Authorization Bypass Through User-Controlled Key vulnerability in CBOT Chatbot allows Authentication Abuse, Authentication Bypass.This issue affects Chatbot: before Core:	N/A	A-CBO-CBOT-020623/81

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v4.0.3.4 Panel: v4.0.3.7. **CVE ID : CVE-2023-2883**		
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	25-May-2023	8.1	Channel Accessible by Non-Endpoint vulnerability in CBOT Chatbot allows Adversary in the Middle (AiTM).This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7. **CVE ID : CVE-2023-2885**	N/A	A-CBO-CBOT-020623/82
N/A	25-May-2023	4.3	Missing Origin Validation in WebSockets vulnerability in CBOT Chatbot allows Content Spoofing Via Application API Manipulation.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7. **CVE ID : CVE-2023-2886**	N/A	A-CBO-CBOT-020623/83
Product: cbot_panel					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 4.0.3.7					
N/A	25-May-2023	9.8	Generation of Incorrect Security Tokens vulnerability in CBOT Chatbot allows Token Impersonation, Privilege Abuse.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7. **CVE ID : CVE-2023-2882**	N/A	A-CBO-CBOT-020623/84
Use of Insufficiently Random Values	25-May-2023	9.8	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG), Use of Insufficiently Random Values vulnerability in CBOT Chatbot allows Signature Spoofing by Key Recreation.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7. **CVE ID : CVE-2023-2884**	N/A	A-CBO-CBOT-020623/85
Authorization Bypass Through	25-May-2023	8.8	Authorization Bypass Through User-Controlled	N/A	A-CBO-CBOT-020623/86

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
User-Controlled Key			Key vulnerability in CBOT Chatbot allows Authentication Abuse, Authentication Bypass.This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7. **CVE ID : CVE-2023-2883**		
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	25-May-2023	8.1	Channel Accessible by Non-Endpoint vulnerability in CBOT Chatbot allows Adversary in the Middle (AiTM).This issue affects Chatbot: before Core: v4.0.3.4 Panel: v4.0.3.7. **CVE ID : CVE-2023-2885**	N/A	A-CBO-CBOT-020623/87
N/A	25-May-2023	4.3	Missing Origin Validation in WebSockets vulnerability in CBOT Chatbot allows Content Spoofing Via Application API Manipulation.This issue affects Chatbot: before	N/A	A-CBO-CBOT-020623/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Core: v4.0.3.4 Panel: v4.0.3.7. **CVE ID : CVE-2023-2886**		
Vendor: cc_custom_taxonomy_project					
Product: cc_custom_taxonomy					
Affected Version(s): * Up to (including) 1.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in chuyencode CC Custom Taxonomy plugin <= 1.0.1 versions. **CVE ID : CVE-2023-25028**	N/A	A-CC_-CC_C-020623/89
Vendor: cdesigner_project					
Product: cdesigner					
Affected Version(s): * Up to (including) 3.2.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-2023	9.8	PrestaShop cdesigner < 3.1.9 is vulnerable to SQL Injection via CdesignerTraitementModuleFrontController::initContent(). **CVE ID : CVE-2023-30191**	https://friends-of-presta.github.io/security-advisories/modules/2023/05/17/cdesigner-89.html	A-CDE-CDES-020623/90
Vendor: churchcrm					
Product: churchcrm					
Affected Version(s): 4.5.4					
Improper Neutralization of	17-May-2023	4.8	ChurchCRM v4.5.4 is vulnerable to Reflected Cross-Site	N/A	A-CHU-CHUR-020623/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			Scripting (XSS) via image file. **CVE ID : CVE-2023-31699**		
Vendor: Cisco					
Product: dna_center					
Affected Version(s): * Up to (excluding) 2.2.3.5					
Files or Directories Accessible to External Parties	18-May-2023	4.3	Multiple vulnerabilities in the API of Cisco DNA Center Software could allow an authenticated, remote attacker to read information from a restricted container, enumerate user information, or execute arbitrary commands in a restricted container as the root user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20184**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-multiple-kTQkGU3	A-CIS-DNA_-020623/92
Affected Version(s): * Up to (excluding) 2.3.3.7					
Improper Input Validation	18-May-2023	8.8	Multiple vulnerabilities in the API of Cisco DNA Center Software could allow an authenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-	A-CIS-DNA_-020623/93

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to read information from a restricted container, enumerate user information, or execute arbitrary commands in a restricted container as the root user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20182**	multiple-kTQkGU3	
Files or Directories Accessible to External Parties	18-May-2023	4.3	Multiple vulnerabilities in the API of Cisco DNA Center Software could allow an authenticated, remote attacker to read information from a restricted container, enumerate user information, or execute arbitrary commands in a restricted container as the root user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20183**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-multiple-kTQkGU3	A-CIS-DNA_-020623/94

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 2.3.4 Up to (excluding) 2.3.5.3					
Improper Input Validation	18-May-2023	8.8	Multiple vulnerabilities in the API of Cisco DNA Center Software could allow an authenticated, remote attacker to read information from a restricted container, enumerate user information, or execute arbitrary commands in a restricted container as the root user. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20182**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-multiple-kTQkGU3	A-CIS-DNA_-020623/95
Files or Directories Accessible to External Parties	18-May-2023	4.3	Multiple vulnerabilities in the API of Cisco DNA Center Software could allow an authenticated, remote attacker to read information from a restricted container, enumerate user information, or execute arbitrary commands in a restricted container as the root user.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-multiple-kTQkGU3	A-CIS-DNA_-020623/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20183**		
Product: identity_services_engine					
Affected Version(s): * Up to (excluding) 3.0.0					
Improper Restriction of XML External Entity Reference	18-May-2023	4.9	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files or conduct a server-side request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20173**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-696OZTCm	A-CIS-IDEN-020623/97
Improper Restriction of XML	18-May-2023	4.9	Multiple vulnerabilities in the web-based	https://sec.cloudapps.cisco.com/security/c	A-CIS-IDEN-020623/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
External Entity Reference			management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files or conduct a server-side request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20174**	enter/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-696OZTCm	
Affected Version(s): * Up to (excluding) 3.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-May-2023	4.9	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform path traversal attacks on the underlying operating system to either elevate privileges to root or read arbitrary files. To exploit these vulnerabilities, an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-traversal-ZTUgMYhu	A-CIS-IDEN-020623/99

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20167**		
Affected Version(s): * Up to (including) 2.7					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-May-2023	7.2	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20163**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-sRQnsEU9	A-CIS-IDEN-020623/100
Improper Neutralization of Special	18-May-2023	7.2	Multiple vulnerabilities in Cisco Identity Services Engine	https://sec.cloudapps.cisco.com/security/center/content	A-CIS-IDEN-020623/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			(ISE) could allow an authenticated attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20164**	/CiscoSecurityAdvisory/cisco-sa-ise-injection-sRQnsEU9	
Affected Version(s): * Up to (including) 3.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-May-2023	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to download arbitrary files from the filesystem of an affected device. These vulnerabilities are due to insufficient input validation. An attacker could exploit these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-dwnld-Srcdnkd2	A-CIS-IDEN-020623/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to download arbitrary files from the underlying filesystem of the affected device. **CVE ID : CVE-2023-20077**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-May-2023	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to download arbitrary files from the filesystem of an affected device. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to download arbitrary files from the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-dwnld-Srcdnkd2	A-CIS-IDEN-020623/103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying filesystem of the affected device. **CVE ID : CVE-2023-20087**		
Affected Version(s): 3.0.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-May-2023	7.2	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20163**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-sRQnsEU9	A-CIS-IDEN-020623/104
Improper Neutralization of Special Elements used in an OS Command ('OS	18-May-2023	7.2	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform command injection attacks on the underlying	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-sRQnsEU9	A-CIS-IDEN-020623/105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20164**		
Improper Restriction of XML External Entity Reference	18-May-2023	4.9	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files or conduct a server-side request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-696OZTCm	A-CIS-IDEN-020623/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20173		
Improper Restriction of XML External Entity Reference	18-May-2023	4.9	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files or conduct a server-side request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20174**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-696OZTCm	A-CIS-IDEN-020623/107
Affected Version(s): 3.1					
Improper Neutralization of Special Elements used in an OS Command ('OS	18-May-2023	7.2	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform command injection attacks on the underlying operating system	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-sRQnsEU9	A-CIS-IDEN-020623/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20163**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-May-2023	7.2	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20164**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-sRQnsEU9	A-CIS-IDEN-020623/109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-May-2023	6.5	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20171**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-delete-read-PK5ghDDd	A-CIS-IDEN-020623/110
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-May-2023	4.9	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform path traversal attacks on the underlying operating system to either elevate privileges to root or read arbitrary files. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-traversal-ZTUgMYhu	A-CIS-IDEN-020623/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20167**		
Improper Input Validation	18-May-2023	4.9	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20172**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-delete-read-PK5ghDDd	A-CIS-IDEN-020623/112
Improper Restriction of XML External Entity Reference	18-May-2023	4.9	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-696OZTCm	A-CIS-IDEN-020623/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			or conduct a server-side request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20173**		
Improper Restriction of XML External Entity Reference	18-May-2023	4.9	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files or conduct a server-side request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-696OZTCm	A-CIS-IDEN-020623/114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20174**		
N/A	18-May-2023	3.8	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20106**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-delete-read-PK5ghDDd	A-CIS-IDEN-020623/115
Affected Version(s): 3.2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-May-2023	7.2	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform command injection attacks on the underlying operating system and elevate privileges to root.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-sRQnsEU9	A-CIS-IDEN-020623/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20163**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-May-2023	7.2	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20164**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-injection-sRQnsEU9	A-CIS-IDEN-020623/117
Improper Limitation of a Pathname	18-May-2023	6.7	Multiple vulnerabilities in Cisco Identity Services Engine	https://sec.cloudapps.cisco.com/security/center/content	A-CIS-IDEN-020623/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			(ISE) could allow an authenticated attacker to perform path traversal attacks on the underlying operating system to either elevate privileges to root or read arbitrary files. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20166**	/CiscoSecurityAdvisory/cisco-sa-ise-traversal-ZTUgMYhu	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-May-2023	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to download arbitrary files from the filesystem of an affected device. These vulnerabilities are due to insufficient input validation. An attacker could exploit these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-dwnld-Srcdnkd2	A-CIS-IDEN-020623/119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to download arbitrary files from the underlying filesystem of the affected device. **CVE ID : CVE-2023-20077**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-May-2023	6.5	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to download arbitrary files from the filesystem of an affected device. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to download arbitrary files from the	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-dwnld-Srcdnkd2	A-CIS-IDEN-020623/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			underlying filesystem of the affected device. **CVE ID : CVE-2023-20087**		
Improper Input Validation	18-May-2023	6.5	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20171**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-delete-read-PK5ghDDd	A-CIS-IDEN-020623/121
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-May-2023	4.9	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform path traversal attacks on the underlying operating system to either elevate privileges to root or read arbitrary files.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-traversal-ZTUgMYhu	A-CIS-IDEN-020623/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20167**		
Improper Input Validation	18-May-2023	4.9	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20172**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-delete-read-PK5ghDDd	A-CIS-IDEN-020623/123
Improper Restriction of XML External	18-May-2023	4.9	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	A-CIS-IDEN-020623/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Entity Reference			Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files or conduct a server-side request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20173**	o-sa-ise-xxe-inj-696OZTCm	
Improper Restriction of XML External Entity Reference	18-May-2023	4.9	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files or conduct a server-side request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xxe-inj-696OZTCm	A-CIS-IDEN-020623/125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20174**		
N/A	18-May-2023	3.8	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20106**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-delete-read-PK5ghDDd	A-CIS-IDEN-020623/126
Product: smart_software_manager_on-prem					
Affected Version(s): * Up to (excluding) 8-202303					
Improper Neutralization of Special Elements used in an SQL	18-May-2023	6.5	A vulnerability in the web-based management interface of Cisco Smart Software Manager On-Prem (SSM On-Prem)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	A-CIS-SMAR-020623/127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface inadequately validates user input. An attacker could exploit this vulnerability by authenticating to the application as a low-privileged user and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to read sensitive data on the underlying database. **CVE ID : CVE-2023-20110**	o-sa-ssm-sql-X9MmjSYh	
Vendor: cityboss					
Product: e-municipality					
Affected Version(s): * Up to (excluding) 6.05					
Improper Neutralization of Special Elements used in an SQL Command	24-May-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cityboss E-municipality allows	N/A	A-CIT-E-MU-020623/128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			SQL Injection.This issue affects E-municipality: before 6.05. **CVE ID : CVE-2023-2750**		
Vendor: Civicrm					
Product: civicrm					
Affected Version(s): 5.59					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Stored Cross Site Scripting (XSS) vulnerability in the add contact function CiviCRM 5.59.alpha1, allows attackers to execute arbitrary code in first/second name field. **CVE ID : CVE-2023-25440**	N/A	A-CIV-CIVI-020623/129
Vendor: class_scheduling_system_project					
Product: class_scheduling_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-May-2023	9.8	A vulnerability was found in SourceCodester Class Scheduling System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/edit_subject.php of the component GET	N/A	A-CLA-CLAS-020623/130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-229597 was assigned to this vulnerability. **CVE ID : CVE-2023-2823**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-2023	6.1	A vulnerability classified as problematic has been found in SourceCodester Class Scheduling System 1.0. Affected is an unknown function of the file /admin/save_teacher.php of the component POST Parameter Handler. The manipulation of the argument Academic_Rank leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this	N/A	A-CLA-CLAS-020623/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-229428. **CVE ID : CVE-2023-2814**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-May-2023	5.4	A vulnerability has been found in SourceCodester Class Scheduling System 1.0 and classified as problematic. This vulnerability affects unknown code of the file search_teacher_result.php of the component POST Parameter Handler. The manipulation of the argument teacher leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229612. **CVE ID : CVE-2023-2826**	N/A	A-CLA-CLAS-020623/132
Vendor: cloudfoundry					
Product: capi-release					
Affected Version(s): From (including) 1.140 Up to (including) 1.152.0					
Improper Certificate Validation	19-May-2023	8.1	Cloud foundry instances having CAPI version between 1.140 and 1.152.0 along with loggregator-agent	https://www.cloudfoundry.org/blog/cve-2023-20881-cas-for-syslog-drain-mtls-	A-CLO-CAPI-020623/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v7+ may override other users syslog drain credentials if they're aware of the client certificate used for that syslog drain. This applies even if the drain has zero certs. This would allow the user to override the private key and add or modify a certificate authority used for the connection. **CVE ID : CVE-2023-20881**	feature-can-be-overwritten/	
Product: cf-deployment					
Affected Version(s): From (including) 24.7.0 Up to (including) 29.0.0					
Improper Certificate Validation	19-May-2023	8.1	Cloud foundry instances having CAPI version between 1.140 and 1.152.0 along with loggregator-agent v7+ may override other users syslog drain credentials if they're aware of the client certificate used for that syslog drain. This applies even if the drain has zero certs. This would allow the user to override the private key and add or modify a certificate authority used for the connection.	https://www.cloudfoundry.org/blog/cve-2023-20881-cas-for-syslog-drain-mtls-feature-can-be-overwritten/	A-CLO-CF-D-020623/134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20881		
Product: loggregator-agent					
Affected Version(s): From (including) 7.0 Up to (including) 7.2.1					
Improper Certificate Validation	19-May-2023	8.1	Cloud foundry instances having CAPI version between 1.140 and 1.152.0 along with loggregator-agent v7+ may override other users syslog drain credentials if they're aware of the client certificate used for that syslog drain. This applies even if the drain has zero certs. This would allow the user to override the private key and add or modify a certificate authority used for the connection. **CVE ID : CVE-2023-20881**	https://www.cloudfoundry.org/blog/cve-2023-20881-cas-for-syslog-drain-mtls-feature-can-be-overwritten/	A-CLO-LOGG-020623/135
Vendor: cloudogu					
Product: scm_manager					
Affected Version(s): From (including) 1.2 Up to (including) 1.60					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in Cloudogu GmbH SCM Manager v1.2 to v1.60 allows attackers to execute arbitrary web scripts or HTML via a crafted payload	N/A	A-CLO-SCM_-020623/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected into the Description text field. **CVE ID : CVE-2023-33829**		
Vendor: Clusterlabs					
Product: pcs					
Affected Version(s): 0.11.4-6.el9					
N/A	17-May-2023	9.8	It was discovered that an update for PCS package in RHBA-2023:2151 erratum released as part of Red Hat Enterprise Linux 9.2 failed to include the fix for the Webpack issue CVE-2023-28154 (for PCS package), which was previously addressed in Red Hat Enterprise Linux 9.1 via erratum RHSA-2023:1591. The CVE-2023-2319 was assigned to that Red Hat specific security regression in Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2319**	N/A	A-CLU-PCS-020623/137
Vendor: cms_tree_page_view_project					
Product: cms_tree_page_view					
Affected Version(s): * Up to (including) 1.6.7					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Jon Christopher CMS Tree Page View plugin <= 1.6.7 versions. **CVE ID : CVE-2023-30868**	N/A	A-CMS-CMS_-020623/138
Vendor: cnoa_oa_project					
Product: cnoa_oa					
Affected Version(s): * Up to (including) 5.1.1.5					
Use of Hard-coded Password	18-May-2023	9.8	A vulnerability, which was classified as problematic, has been found in cnoa OA up to 5.1.1.5. Affected by this issue is some unknown functionality of the file /index.php?app=main&func=passport&action=login. The manipulation leads to use of hard-coded password. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229376. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-CNO-CNOA-020623/139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2799		
Vendor: comment_system_project					
Product: comment_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-May-2023	6.1	A vulnerability classified as problematic has been found in SourceCodester Comment System 1.0. Affected is an unknown function of the file index.php of the component GET Parameter Handler. The manipulation of the argument msg leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-230076. **CVE ID : CVE-2023-2922**	N/A	A-COM-COMM-020623/140
Vendor: conlabz					
Product: wp_google_tag_manager					
Affected Version(s): * Up to (including) 1.1					
Cross-Site Request Forgery (CSRF)	26-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in conlabzgmbh WP Google Tag	N/A	A-CON-WP_G-020623/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Manager plugin <= 1.1 versions. **CVE ID : CVE-2023-22693**		
Vendor: content_management_system_project					
Product: content_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-May-2023	6.1	IT Sourcecode Content Management System Project In PHP and MySQL With Source Code 1.0.0 is vulnerable to Cross Site Scripting (XSS) via /ecodesource/search_list.php. **CVE ID : CVE-2023-31816**	N/A	A-CON-CONT-020623/142
Vendor: Craftcms					
Product: craft_cms					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.4.6					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-May-2023	7.2	Craft CMS is an open source content management system. In affected versions of Craft CMS an unrestricted file extension may lead to Remote Code Execution. If the name parameter value is not empty string('') in the View.php's doesTemplateExist() -> resolveTemplate() -	https://github.com/craftcms/cms/security/advisories/GHSA-vqxf-r9ph-cc9c	A-CRA-CRAF-020623/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			> _resolveTemplateInternal() -> _resolveTemplate() function, it returns directly without extension verification, so that arbitrary extension files are rendered as twig templates. When attacker with admin privileges on a DEV or an improperly configured STG or PROD environment, they can exploit this vulnerability to remote code execution. Code execution may grant the attacker access to the host operating system. This issue has been addressed in version 4.4.6. Users are advised to upgrade. There are no known workarounds for this vulnerability. **CVE ID : CVE-2023-32679**		
Vendor: crmperks					
Product: contact_form_entries_-_contact_form_7_wpforms_and_more					
Affected Version(s): * Up to (including) 1.3.0					
Improper Neutralization of Input	28-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS)	N/A	A-CRM-CONT-020623/144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerability in CRM Perks Contact Form Entries plugin <= 1.3.0 versions. **CVE ID : CVE-2023-33311**		
Product: integration_for_contact_form_7_and_zoho_crm\,_bigin					
Affected Version(s): * Up to (including) 1.2.2					
Cross-Site Request Forgery (CSRF)	26-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in CRM Perks Integration for Contact Form 7 and Zoho CRM, Bigin plugin <= 1.2.2 versions. **CVE ID : CVE-2023-25976**	N/A	A-CRM-INTE-020623/145
Vendor: custom_field_suite_project					
Product: custom_field_suite					
Affected Version(s): * Up to (excluding) 2.6.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Matt Gibbs Custom Field Suite plugin <= 2.6.2.1 versions. **CVE ID : CVE-2023-32515**	N/A	A-CUS-CUST-020623/146
Vendor: Cybozu					
Product: garoon					
Affected Version(s): 5.15.0					
N/A	23-May-2023	4.3	Operation restriction bypass vulnerability in MultiReport of Cybozu Garoon	https://cs.cybozu.co.jp/2023/007698.html	A-CYB-GARO-020623/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			5.15.0 allows a remote authenticated attacker to alter the data of MultiReport. **CVE ID : CVE-2023-27384**		
Affected Version(s): From (including) 4.10.0 Up to (including) 5.9.2					
Uncontrolled Resource Consumption	23-May-2023	6.5	Denial-of-service (DoS) vulnerability in Message of Cybozu Garoon 4.10.0 to 5.9.2 allows a remote authenticated attacker to cause a denial of service condition. **CVE ID : CVE-2023-26595**	https://cs.cybozu.co.jp/2023/007698.html	A-CYB-GARO-020623/148
Affected Version(s): From (including) 4.6.0 Up to (including) 5.9.2					
N/A	23-May-2023	4.3	Operation restriction bypass vulnerability in Message and Bulletin of Cybozu Garoon 4.6.0 to 5.9.2 allows a remote authenticated attacker to alter the data of Message and/or Bulletin. **CVE ID : CVE-2023-27304**	https://cs.cybozu.co.jp/2023/007698.html	A-CYB-GARO-020623/149
Vendor: davinci_project					
Product: davinci					
Affected Version(s): 0.3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	17-May-2023	8.8	davinci 0.3.0-rc is vulnerable to Server-side request forgery (SSRF). **CVE ID : CVE-2023-31848**	N/A	A-DAV-DAVI-020623/150
N/A	17-May-2023	6.5	In davinci 0.3.0-rc after logging in, the user can connect to the mysql malicious server by controlling the data source to read arbitrary files on the client side. **CVE ID : CVE-2023-31847**	N/A	A-DAV-DAVI-020623/151
Vendor: Dedecms					
Product: dedecms					
Affected Version(s): 5.7.108					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-2023	5.4	DedeCMS up to v5.7.108 is vulnerable to XSS in sys_info.php via parameters 'edit__cfg_powerby' and 'edit__cfg_beian' **CVE ID : CVE-2023-31757**	N/A	A-DED-DEDE-020623/152
Vendor: Dell					
Product: cloudiq_collector					
Affected Version(s): From (including) 1.10.2 Up to (excluding) 1.10.17					
Missing Encryption of Sensitive Data	19-May-2023	7.1	Dell CloudIQ Collector version 1.10.2 contains a missing encryption of sensitive data vulnerability. An	https://www.dell.com/support/kbdoc/en-us/000213696/dsa-2023-165-dell-cloudiq-	A-DEL-CLOU-020623/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker with low privileges could potentially exploit this vulnerability, leading to gain access to unauthorized data. **CVE ID : CVE-2023-28045**	collector-security-update-for-missing-encryption-of-sensitive-data-vulnerability	
Product: cloudlink					
Affected Version(s): * Up to (excluding) 7.1.3					
Use of a Broken or Risky Cryptographic Algorithm	16-May-2023	7.5	CloudLink 7.1.2 and all prior versions contain a broken or risky cryptographic algorithm vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability leading to some information disclosure. **CVE ID : CVE-2023-28076**	https://www.dell.com/support/kbdoc/en-us/000212095/dsa-2023-121-dell-cloudlink-security-update-for-aes-gcm-ciphers-vulnerability	A-DEL-CLOU-020623/154
Vendor: dental_clinic_appointment_reservation_system_project					
Product: dental_clinic_appointment_reservation_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation	20-May-2023	6.1	A vulnerability was found in SourceCodester Dental Clinic Appointment Reservation System 1.0. It has been	N/A	A-DEN-DENT-020623/155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			rated as problematic. Affected by this issue is some unknown functionality of the file /admin/service.php of the component POST Parameter Handler. The manipulation of the argument service leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-229598 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-2824**		
Vendor: dgraph					
Product: dgraph					
Affected Version(s): * Up to (excluding) 23.0.0					
Inadequate Encryption Strength	17-May-2023	5.5	Dgraph is an open source distributed GraphQL database. Existing Dgraph audit logs are vulnerable to brute force attacks due to nonce collisions. The first 12 bytes come from a baseIv which is initialized when an audit log is	https://github.com/dgraph-io/dgraph/security/advisories/GHSA-92wq-q9pq-gw47, https://github.com/dgraph-io/dgraph/pull/8323	A-DGR-DGRA-020623/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			created. The last 4 bytes come from the length of the log line being encrypted. This is problematic because two log lines will often have the same length, so due to these collisions we are reusing the same nonce many times. All audit logs generated by versions of Dgraph <v23.0.0 are affected. Attackers must have access to the system the logs are stored on. Dgraph users should upgrade to v23.0.0. Users unable to upgrade should store existing audit logs in a secure location and for extra security, encrypt using an external tool like `gpg`. **CVE ID : CVE-2023-31135**		
Vendor: dogblocker					
Product: minify_html					
Affected Version(s): * Up to (including) 2.1.7					
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Tim Eckel Minify HTML	N/A	A-DOG-MINI-020623/157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin <= 2.1.7 vulnerability. **CVE ID : CVE-2023-26014**		
Product: read_more_excerpt_link					
Affected Version(s): * Up to (including) 1.6					
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Tim Eckel Read More Excerpt Link plugin <= 1.6 versions. **CVE ID : CVE-2023-26011**	N/A	A-DOG-READ-020623/158
Vendor: easyimages2.0_project					
Product: easyimages2.0					
Affected Version(s): * Up to (excluding) 2.8.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	6.1	EasyImages2.0 ? 2.8.1 is vulnerable to Cross Site Scripting (XSS) via viewlog.php. **CVE ID : CVE-2023-33599**	https://github.com/icret/EasyImages2.0/issues/115	A-EAS-EASY-020623/159
Vendor: Eclipse					
Product: openj9					
Affected Version(s): * Up to (excluding) 0.38.0					
Out-of-bounds Read	22-May-2023	9.1	In Eclipse Openj9 before version 0.38.0, in the implementation of the shared cache (which is enabled by default in OpenJ9 builds) the size of a string is not properly	https://github.com/eclipse-openj9/openj9/pull/17259	A-ECL-OPEN-020623/160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			checked against the size of the buffer. **CVE ID : CVE-2023-2597**		
Vendor: electronic					
Product: flexihub					
Affected Version(s): 5.5.14691.0					
NULL Pointer Dereference	24-May-2023	5.5	A vulnerability classified as problematic has been found in FlexiHub 5.5.14691.0. This affects the function 0x220088 in the library fusbhub.sys of the component IoControlCode Handler. The manipulation leads to null pointer dereference. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-229851. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2872**	N/A	A-ELE-FLEX-020623/161
Vendor: ellucian					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ethos_identity					
Affected Version(s): * Up to (excluding) 5.10.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-2023	6.1	A vulnerability was found in Ellucian Ethos Identity up to 5.10.5. It has been classified as problematic. Affected is an unknown function of the file /cas/logout. The manipulation of the argument url leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 5.10.6 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-229596. **CVE ID : CVE-2023-2822**	N/A	A-ELL-ETHO-020623/162
Vendor: employee_and_visitor_gate_pass_logging_system_project					
Product: employee_and_visitor_gate_pass_logging_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements	23-May-2023	9.8	SourceCodester Employee and Visitor Gate Pass Logging System v1.0 is vulnerable	N/A	A-EMP-EMPL-020623/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			to SQL Injection via /employee_gatepass/classes/Login.php. **CVE ID : CVE-2023-31752**		
Vendor: Entechtaiwan					
Product: monitor_asset_manager					
Affected Version(s): 2.9					
Improper Resource Shutdown or Release	24-May-2023	5.5	A vulnerability was found in EnTech Monitor Asset Manager 2.9. It has been declared as problematic. Affected by this vulnerability is the function 0x80002014 of the component IoControlCode Handler. The manipulation leads to denial of service. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The identifier VDB-229849 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-ENT-MONI-020623/164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2870		
Vendor: escanav					
Product: escan_anti-virus					
Affected Version(s): 22.0.1400.2443					
NULL Pointer Dereference	24-May-2023	5.5	A vulnerability, which was classified as problematic, was found in eScan Antivirus 22.0.1400.2443. Affected is the function 0x22E008u in the library PROCOBSRVESX.SYS of the component IoControlCode Handler. The manipulation leads to null pointer dereference. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-229854 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2875**	N/A	A-ESC-ESCA-020623/165
Product: escan_management_console					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 14.0.1400.2281					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	9	Cross Site Scripting (XSS) in the edit user form in Microworld Technologies eScan management console 14.0.1400.2281 allows remote attacker to inject arbitrary code via the from parameter. **CVE ID : CVE-2023-31703**	N/A	A-ESC-ESCA-020623/166
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-2023	7.2	SQL injection in the View User Profile in MicroWorld eScan Management Console 14.0.1400.2281 allows remote attacker to dump entire database and gain windows XP command shell to perform code execution on database server via GetUserCurrentPwd?UsrId=1. **CVE ID : CVE-2023-31702**	N/A	A-ESC-ESCA-020623/167
Vendor: exelysis					
Product: exelysis_unified_communications_solution					
Affected Version(s): 1.0					
Improper Neutralization of Input	17-May-2023	6.1	Cross Site Scripting vulnerability found in Exelysis Unified Communication	N/A	A-EXE-EXEL-020623/168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Solution (EUCS) v.1.0 allows a remote attacker to gain privileges via the URL path of the eucsAdmin login web page. **CVE ID : CVE-2023-29837**		
Vendor: eyoucms					
Product: eyoucms					
Affected Version(s): 1.6.2					
Cross-Site Request Forgery (CSRF)	23-May-2023	4.3	A Cross-Site Request Forgery (CSRF) in EyouCMS v1.6.2 allows attackers to execute arbitrary commands via a supplying a crafted HTML file to the Upload software format function. **CVE ID : CVE-2023-31708**	N/A	A-EYO-EYOU-020623/169
Vendor: fabulatech					
Product: usb_for_remote_desktop					
Affected Version(s): 6.1.0.0					
NULL Pointer Dereference	24-May-2023	5.5	A vulnerability was found in FabulaTech USB for Remote Desktop 6.1.0.0. It has been rated as problematic. Affected by this issue is the function 0x220448/0x220420/0x22040c/0x220408 of the component	N/A	A-FAB-USB_-020623/170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IoControlCode Handler. The manipulation leads to null pointer dereference. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. VDB-229850 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2871**		
Vendor: Facebook					
Product: fizz					
Affected Version(s): * Up to (excluding) 2023.01.30.00					
Reachable Assertion	18-May-2023	7.5	There is a vulnerability in the fizz library prior to v2023.01.30.00 where a CHECK failure can be triggered remotely. This behavior requires the client supported cipher advertisement changing between the original ClientHello and the second ClientHello, crashing the	https://www.facebook.com/security/advisories/cve-2023-23759, https://github.com/facebookincubator/fizz/commit/8d3649841597bedfb6986c30431ebad0eb215265	A-FAC-FIZZ-020623/171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process (impact is limited to denial of service). **CVE ID : CVE-2023-23759**		
Product: hermes					
Affected Version(s): -					
Access of Resource Using Incompatible Type ('Type Confusion')	18-May-2023	9.8	A type confusion bug in TypedArray prior to commit e6ed9c1a4b02dc219de1648f44cd808a56171b81 could have been used by a malicious attacker to execute arbitrary code via untrusted JavaScript. Note that this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected. **CVE ID : CVE-2023-25933**	https://github.com/facebook/hermes/commit/e6ed9c1a4b02dc219de1648f44cd808a56171b81, https://www.facebook.com/security/advisories/cve-2023-25933	A-FAC-HERM-020623/172
Use After Free	18-May-2023	9.8	A bytecode optimization bug in Hermes prior to commit e6ed9c1a4b02dc219de1648f44cd808a56171b81 could be used to cause an use-after-free and obtain arbitrary code execution via a carefully crafted payload. Note that	https://github.com/facebook/hermes/commit/e6ed9c1a4b02dc219de1648f44cd808a56171b81, https://www.facebook.com/security/advisories/cve-2023-28081	A-FAC-HERM-020623/173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected. **CVE ID : CVE-2023-28081**		
Use After Free	18-May-2023	9.8	A use-after-free related to unsound inference in the bytecode generation when optimizations are enabled for Hermes prior to commit da8990f737ebb9d9810633502f65ed462b819c09 could have been used by an attacker to achieve remote code execution. Note that this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected. **CVE ID : CVE-2023-30470**	https://www.facebook.com/security/advisories/cve-2023-30470, https://github.com/facebook/hermes/commit/da8990f737ebb9d9810633502f65ed462b819c09	A-FAC-HERM-020623/174
Affected Version(s): * Up to (excluding) 2023-01-10					
Access of Resource Using Incompatib	18-May-2023	9.8	An error in Hermes' algorithm for copying objects properties prior to	https://github.com/facebook/hermes/commit/a00d23	A-FAC-HERM-020623/175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
le Type ('Type Confusion')			commit a00d237346894c6067a594983be6634f4168c9ad could be used by a malicious attacker to execute arbitrary code via type confusion. Note that this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected. **CVE ID : CVE-2023-23557**	7346894c6067a594983be6634f4168c9ad, https://www.facebook.com/security/advisories/cve-2023-23557	
Affected Version(s): * Up to (excluding) 2023-01-31					
NULL Pointer Dereference	18-May-2023	7.5	A null pointer dereference bug in Hermes prior to commit 5cae9f72975cf0e5a62b27fdd8b01f103e198708 could have been used by an attacker to crash an Hermes runtime where the EnableHermesInternal config option was set to true. Note that this is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native	https://www.facebook.com/security/advisories/cve-2023-24832, https://github.com/facebook/hermes/commit/5cae9f72975cf0e5a62b27fdd8b01f103e198708	A-FAC-HERM-020623/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			applications are not affected. **CVE ID : CVE-2023-24832**		
Affected Version(s): * Up to (excluding) 2023-02-02					
Out-of-bounds Write	18-May-2023	9.8	An error in BigInt conversion to Number in Hermes prior to commit a6dcafe6ded8e61658b40f5699878cd19a481f80 could have been used by a malicious attacker to execute arbitrary code due to an out-of-bound write. Note that this bug is only exploitable in cases where Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected. **CVE ID : CVE-2023-23556**	https://github.com/facebook/hermes/commit/a6dcafe6ded8e61658b40f5699878cd19a481f80, https://www.facebook.com/security/advisories/cve-2023-23556	A-FAC-HERM-020623/177
Use After Free	18-May-2023	7.5	A use-after-free in BigIntPrimitive addition in Hermes prior to commit a6dcafe6ded8e61658b40f5699878cd19a481f80 could have been used by an attacker to leak raw data from Hermes VM's heap. Note that this is only exploitable in cases where	https://github.com/facebook/hermes/commit/a6dcafe6ded8e61658b40f5699878cd19a481f80, https://www.facebook.com/security/advisories/cve-2023-24833	A-FAC-HERM-020623/178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Hermes is used to execute untrusted JavaScript. Hence, most React Native applications are not affected. **CVE ID : CVE-2023-24833**		
Product: netconsd					
Affected Version(s): 0.1					
Out-of-bounds Write	18-May-2023	9.8	netconsd prior to v0.2 was vulnerable to an integer overflow in its parse_packet function. A malicious individual could leverage this overflow to create heap memory corruption with attacker controlled data. **CVE ID : CVE-2023-28753**	https://www.facebook.com/security/advisories/cve-2023-28753, https://github.com/facebook/netconsd/commit/9fc54edf54f7caea1189c2b979337ed37af2c60e	A-FAC-NETC-020623/179
Vendor: faculty_evaluation_system_project					
Product: faculty_evaluation_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-May-2023	7.2	Sourcecodester Faculty Evaluation System v1.0 is vulnerable to SQL Injection via /eval/admin/manage_task.php?id=. **CVE ID : CVE-2023-33439**	N/A	A-FAC-FACU-020623/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	26-May-2023	7.2	Sourcecodester Faculty Evaluation System v1.0 is vulnerable to arbitrary code execution via /eval/ajax.php?action=save_user. **CVE ID : CVE-2023-33440**	N/A	A-FAC-FACU-020623/181
Vendor: file_gallery_project					
Product: file_gallery					
Affected Version(s): * Up to (excluding) 1.8.5.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Bruno "Aesqe" Babic File Gallery plugin <= 1.8.5.3 versions. **CVE ID : CVE-2023-23676**	N/A	A-FIL-FILE-020623/182
Vendor: Filseclab					
Product: twister_antivirus					
Affected Version(s): From (including) 8.0 Up to (including) 8.17					
Out-of-bounds Write	24-May-2023	7.8	A vulnerability classified as critical was found in Twister Antivirus 8. This vulnerability affects the function 0x804f2143/0x804f217f/0x804f214b/0x80800043 in the library filppd.sys of the component IoControlCode Handler. The manipulation leads	N/A	A-FIL-TWIS-020623/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to memory corruption. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229852. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2873**		
N/A	24-May-2023	5.5	A vulnerability, which was classified as problematic, has been found in Twister Antivirus 8. This issue affects the function 0x804f2158/0x804f2154/0x804f2150/0x804f215c/0x804f2160/0x80800040/0x804f214c/0x804f2148/0x804f2144/0x801120e4/0x804f213c/0x804f2140 in the library filppd.sys of the component IoControlCode Handler. The manipulation leads to denial of service. Attacking locally is	N/A	A-FIL-TWIS-020623/184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-229853 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2874**		
Vendor: finexmedia					
Product: competition_management_system					
Affected Version(s): * Up to (excluding) 23.07					
Authorization Bypass Through User-Controlled Key	23-May-2023	8.8	Authorization Bypass Through User-Controlled Key vulnerability in Finex Media Competition Management System allows Authentication Abuse, Authentication Bypass.This issue affects Competition Management System: before 23.07. **CVE ID : CVE-2023-2702**	N/A	A-FIN-COMP-020623/185
Exposure of	23-May-2023	7.5	Exposure of Private Personal	N/A	A-FIN-COMP-020623/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			Information to an Unauthorized Actor vulnerability in Finex Media Competition Management System allows Retrieve Embedded Sensitive Data, Collect Data as Provided by Users.This issue affects Competition Management System: before 23.07. **CVE ID : CVE-2023-2703**		
Vendor: fit2cloud					
Product: cloudexplorer_lite					
Affected Version(s): * Up to (excluding) 1.1.0					
N/A	23-May-2023	8.1	Improper Access Control in GitHub repository cloudexplorer-dev/cloudexplorer-lite prior to v1.1.0. **CVE ID : CVE-2023-2845**	https://huntr.dev/bounties/ac10e81c-998e-4425-9d74-b985d9b0254c, https://github.com/cloudexplorer-dev/cloudexplorer-lite/commit/d9f55a44e579d312977b02317b2020de758b763a	A-FIT-CLOU-020623/187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authorization Bypass Through User-Controlled Key	23-May-2023	4.9	Missing Authorization in GitHub repository cloudexplorer-dev/cloudexplorer-lite prior to v1.1.0. **CVE ID : CVE-2023-2844**	https://huntr.dev/bounties/6644b36e-603d-4dbe-8ee2-5df8b8fb2e22, https://github.com/cloudexplorer-dev/cloudexplorer-lite/commit/d9f55a44e579d312977b02317b2020de758b763a	A-FIT-CLOU-020623/188
Vendor: fixbd					
Product: educare					
Affected Version(s): * Up to (including) 1.4.1					
Cross-Site Request Forgery (CSRF)	26-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in FixBD Educare plugin <= 1.4.1 versions. **CVE ID : CVE-2023-25971**	N/A	A-FIX-EDUC-020623/189
Vendor: fooplugins					
Product: foogallery					
Affected Version(s): * Up to (including) 2.2.35					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in FooPlugins FooGallery plugin <= 2.2.35 versions. **CVE ID : CVE-2023-29439**	N/A	A-FOO-FOOG-020623/190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: formilla					
Product: live_chat					
Affected Version(s): * Up to (excluding) 1.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Formilla Live Chat by Formilla plugin <= 1.3 versions. **CVE ID : CVE-2023-23727**	N/A	A-FOR-LIVE-020623/191
Vendor: Foxit					
Product: pdf_editor					
Affected Version(s): * Up to (including) 10.1.11.37866					
N/A	19-May-2023	7.8	Foxit PDF Reader (12.1.1.15289 and earlier) and Foxit PDF Editor (12.1.1.15289 and all previous 12.x versions, 11.2.5.53785 and all previous 11.x versions, and 10.1.11.37866 and earlier) on Windows allows Local Privilege Escalation when installed to a non-default directory because unprivileged users have access to an executable file of a system service. This is fixed in 12.1.2. **CVE ID : CVE-2023-33240**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-020623/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 11.0.0 Up to (including) 11.2.5.53785					
N/A	19-May-2023	7.8	Foxit PDF Reader (12.1.1.15289 and earlier) and Foxit PDF Editor (12.1.1.15289 and all previous 12.x versions, 11.2.5.53785 and all previous 11.x versions, and 10.1.11.37866 and earlier) on Windows allows Local Privilege Escalation when installed to a non-default directory because unprivileged users have access to an executable file of a system service. This is fixed in 12.1.2. **CVE ID : CVE-2023-33240**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-020623/193
Affected Version(s): From (including) 12.0.0 Up to (including) 12.1.1.15289					
N/A	19-May-2023	7.8	Foxit PDF Reader (12.1.1.15289 and earlier) and Foxit PDF Editor (12.1.1.15289 and all previous 12.x versions, 11.2.5.53785 and all previous 11.x versions, and 10.1.11.37866 and earlier) on Windows allows Local Privilege Escalation when	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-020623/194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			installed to a non-default directory because unprivileged users have access to an executable file of a system service. This is fixed in 12.1.2. **CVE ID : CVE-2023-33240**		
Product: pdf_reader					
Affected Version(s): * Up to (including) 12.1.1.15289					
N/A	19-May-2023	7.8	Foxit PDF Reader (12.1.1.15289 and earlier) and Foxit PDF Editor (12.1.1.15289 and all previous 12.x versions, 11.2.5.53785 and all previous 11.x versions, and 10.1.11.37866 and earlier) on Windows allows Local Privilege Escalation when installed to a non-default directory because unprivileged users have access to an executable file of a system service. This is fixed in 12.1.2. **CVE ID : CVE-2023-33240**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PDF_-020623/195
Vendor: Freeguppy					
Product: guppy					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 6.00.10					
Unrestricted Upload of File with Dangerous Type	17-May-2023	9.8	GuppY CMS 6.00.10 is vulnerable to Unrestricted File Upload which allows remote attackers to execute arbitrary code by uploading a php file. **CVE ID : CVE-2023-31903**	N/A	A-FRE-GUPP-020623/196
Vendor: Garmin					
Product: connect-iq					
Affected Version(s): From (including) 1.0.0 Up to (including) 4.1.7					
Out-of-bounds Read	23-May-2023	9.8	The `news` MonkeyC operation code in CIQ API version 1.0.0 through 4.1.7 fails to check that string resources are not extending past the end of the expected sections. A malicious CIQ application could craft a string that starts near the end of a section, and whose length extends past its end. Upon loading the string, the GarminOS TVM component may read out-of-bounds memory. **CVE ID : CVE-2023-23301**	N/A	A-GAR-CONN-020623/197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-May-2023	9.8	The GarminOS TVM component in CIQ API version 1.0.0 through 4.1.7 is vulnerable to various buffer overflows when loading binary resources. A malicious application embedding specially crafted resources could hijack the execution of the device's firmware. **CVE ID : CVE-2023-23305**	N/A	A-GAR-CONN-020623/198
N/A	23-May-2023	7.5	The permission system implemented and enforced by the GarminOS TVM component in CIQ API version 1.0.0 through 4.1.7 can be bypassed entirely. A malicious application with specially crafted code and data sections could access restricted CIQ modules, call their functions and disclose sensitive data such as user profile information and GPS coordinates, among others.	N/A	A-GAR-CONN-020623/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23299		
Affected Version(s): From (including) 1.2.0 Up to (including) 4.1.7					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-May-2023	9.8	The `Toybox.GenericChannel.setDeviceConfig` API method in CIQ API version 1.2.0 through 4.1.7 does not validate its parameter, which can result in buffer overflows when copying various attributes. A malicious application could call the API method with specially crafted object and hijack the execution of the device's firmware. **CVE ID : CVE-2023-23302**	N/A	A-GAR-CONN-020623/200
Affected Version(s): From (including) 2.1.0 Up to (including) 4.1.7					
N/A	23-May-2023	9.1	The GarminOS TVM component in CIQ API version 2.1.0 through 4.1.7 allows applications with a specially crafted head section to use the `Toybox.SensorHistory` module without permission. A malicious application could call any functions from the	N/A	A-GAR-CONN-020623/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`Toybox.SensorHistory` module without the user's consent and disclose potentially private or sensitive information. **CVE ID : CVE-2023-23304**		
Affected Version(s): From (including) 2.2.0 Up to (including) 4.1.7					
Out-of-bounds Write	23-May-2023	9.8	The `Toybox.Ant.BurstPayload.add` API method in CIQ API version 2.2.0 through 4.1.7 suffers from a type confusion vulnreability, which can result in an out-of-bounds write operation. A malicious application could create a specially crafted `Toybox.Ant.BurstPayload` object, call its `add` method, override arbitrary memory and hijack the execution of the device's firmware. **CVE ID : CVE-2023-23306**	N/A	A-GAR-CONN-020623/202
Affected Version(s): From (including) 2.3.0 Up to (including) 4.1.7					
Integer Overflow or Wraparound	23-May-2023	9.8	The `Toybox.Graphics.BufferedBitmap.initialize` API method in CIQ API version 2.3.0 through 4.1.7	N/A	A-GAR-CONN-020623/203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			does not validate its parameters, which can result in integer overflows when allocating the underlying bitmap buffer. A malicious application could call the API method with specially crafted parameters and hijack the execution of the device's firmware. **CVE ID : CVE-2023-23298**		
Affected Version(s): From (including) 3.0.0 Up to (including) 4.1.7					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-May-2023	9.8	The `Toybox.Cryptography.Cipher.initialize` API method in CIQ API version 3.0.0 through 4.1.7 does not validate its parameters, which can result in buffer overflows when copying data. A malicious application could call the API method with specially crafted parameters and hijack the execution of the device's firmware. **CVE ID : CVE-2023-23300**	N/A	A-GAR-CONN-020623/204
Affected Version(s): From (including) 3.2.0 Up to (including) 4.1.7					
Buffer Copy without	23-May-2023	9.8	The `Toybox.Ant.GenericChannel.enableEnc	N/A	A-GAR-CONN-020623/205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			ryption` API method in CIQ API version 3.2.0 through 4.1.7 does not validate its parameter, which can result in buffer overflows when copying various attributes. A malicious application could call the API method with specially crafted object and hijack the execution of the device's firmware. **CVE ID : CVE-2023-23303**		
Vendor: getvideostream					
Product: videostream					
Affected Version(s): 0.4.3					
Time-of-check Time-of-use (TOCTOU) Race Condition	17-May-2023	7	Videostream macOS app 0.5.0 and 0.4.3 has a Race Condition. The Updater privileged script attempts to update Videostream every 5 hours. **CVE ID : CVE-2023-25394**	N/A	A-GET-VIDE-020623/206
Affected Version(s): 0.5.0					
Time-of-check Time-of-use (TOCTOU)	17-May-2023	7	Videostream macOS app 0.5.0 and 0.4.3 has a Race Condition. The Updater privileged script attempts to	N/A	A-GET-VIDE-020623/207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Race Condition			update Videostream every 5 hours. **CVE ID : CVE-2023-25394**		
Vendor: Gitlab					
Product: gitlab					
Affected Version(s): 16.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-May-2023	7.5	An issue has been discovered in GitLab CE/EE affecting only version 16.0.0. An unauthenticated malicious user can use a path traversal vulnerability to read arbitrary files on the server when an attachment exists in a public project nested within at least five groups. **CVE ID : CVE-2023-2825**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2825.json	A-GIT-GITL-020623/208
Vendor: glazedlists					
Product: glazed_lists					
Affected Version(s): 1.11.0					
Deserialization of Untrusted Data	16-May-2023	9.8	An XML Deserialization vulnerability in glazedlists v1.11.0 allows an attacker to execute arbitrary code via the BeanXMLByteCoder.decode() parameter.	N/A	A-GLA-GLAZ-020623/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31890		
Vendor: GNU					
Product: binutils					
Affected Version(s): * Up to (including) 2.40					
Out-of-bounds Write	17-May-2023	6.5	A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf.c. This may lead to loss of availability. **CVE ID : CVE-2023-1972**	https://sourceware.org/bugzilla/show_bug.cgi?id=30285	A-GNU-BINU-020623/210
Product: cflow					
Affected Version(s): 1.7					
Improper Resource Shutdown or Release	18-May-2023	7.5	A vulnerability was found in GNU cflow 1.7. It has been rated as problematic. This issue affects the function func_body/parse_variable_declaration of the file parser.c. The manipulation leads to denial of service. The exploit has been disclosed to the public and may be used. The identifier VDB-229373 was assigned to this vulnerability. NOTE: The vendor was contacted early about this	N/A	A-GNU-CFLO-020623/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			disclosure but did not respond in any way. **CVE ID : CVE-2023-2789**		
Product: emacs					
Affected Version(s): 26.1-9.el8					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	7.8	A flaw was found in the Emacs text editor. Processing a specially crafted org-mode code with the "org-babel-execute:latex" function in ob-latex.el can result in arbitrary command execution. This CVE exists because of a CVE-2023-28617 security regression for the emacs package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2491**	N/A	A-GNU-EMAC-020623/212
Affected Version(s): 27.2-8.el9					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	7.8	A flaw was found in the Emacs text editor. Processing a specially crafted org-mode code with the "org-babel-execute:latex" function in ob-latex.el can result in arbitrary command	N/A	A-GNU-EMAC-020623/213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution. This CVE exists because of a CVE-2023-28617 security regression for the emacs package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2491**		
Vendor: Google					
Product: chrome					
Affected Version(s): * Up to (excluding) 113.0.5672.126					
Use After Free	16-May-2023	8.8	Use after free in Navigation in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) **CVE ID : CVE-2023-2721**	N/A	A-GOO-CHRO-020623/214
Use After Free	16-May-2023	8.8	Use after free in Autofill UI in Google Chrome on Android prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium	N/A	A-GOO-CHRO-020623/215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: High) **CVE ID : CVE-2023-2722**		
Use After Free	16-May-2023	8.8	Use after free in DevTools in Google Chrome prior to 113.0.5672.126 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2723**	N/A	A-GOO-CHRO-020623/216
Access of Resource Using Incompatible Type ('Type Confusion')	16-May-2023	8.8	Type confusion in V8 in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2724**	N/A	A-GOO-CHRO-020623/217
Use After Free	16-May-2023	8.8	Use after free in Guest View in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a	N/A	A-GOO-CHRO-020623/218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2725**		
N/A	16-May-2023	8.8	Inappropriate implementation in WebApp Installs in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious web app to bypass install dialog via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2726**	N/A	A-GOO-CHRO-020623/219
Vendor: gpac					
Product: gpac					
Affected Version(s): * Up to (excluding) 2.2.1					
NULL Pointer Dereference	22-May-2023	9.8	NULL Pointer Dereference in GitHub repository gpac/gpac prior to 2.2.2. **CVE ID : CVE-2023-2840**	https://huntr.dev/bounties/21926fc2-6eb1-4e24-8a36-e60f487d0257, https://github.com/gpac/gpac/commit/ba59206b3225f	A-GPA-GPAC-020623/220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				0e8e95a27eff41cb1c49ddf9a37	
Affected Version(s): * Up to (excluding) 2.2.2					
Out-of-bounds Read	22-May-2023	9.1	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.2.2. **CVE ID : CVE-2023-2838**	https://github.com/gpac/gpac/commit/c88df2e202efad214c25b4e586f243b2038779ba, https://huntr.dev/bounties/711e0988-5345-4c01-a2fe-1179604dd07f	A-GPA-GPAC-020623/221
Divide By Zero	22-May-2023	7.5	Divide By Zero in GitHub repository gpac/gpac prior to 2.2.2. **CVE ID : CVE-2023-2839**	https://huntr.dev/bounties/42dce889-f63d-4ea9-970f-1f20fc573d5f, https://github.com/gpac/gpac/commit/047f96fb39e6bf70cb9f344093f5886e51dce0ac	A-GPA-GPAC-020623/222
Stack-based Buffer Overflow	22-May-2023	5.5	Stack-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.2.2. **CVE ID : CVE-2023-2837**	https://github.com/gpac/gpac/commit/6f28c4cd607d83ce381f9b4a9f8101ca1e79c611, https://huntr.dev/bounties/a6bfd1b2-aba8-4c6f-90c4-	A-GPA-GPAC-020623/223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				e95b1831cb17	
Vendor: granthweb					
Product: go_pricing					
Affected Version(s): * Up to (including) 3.3.19					
Missing Authorization	24-May-2023	8.8	The Go Pricing - WordPress Responsive Pricing Tables plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'process_postdata' function in versions up to, and including, 3.3.19. This makes it possible for authenticated attackers with a role that the administrator previously granted access to the plugin to modify access to the plugin when it should only be the administrator's privilege. **CVE ID : CVE-2023-2494**	N/A	A-GRA-GO_P-020623/224
Deserialization of Untrusted Data	25-May-2023	8.8	The Go Pricing - WordPress Responsive Pricing Tables plugin for WordPress is vulnerable to PHP Object Injection in	N/A	A-GRA-GO_P-020623/225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions up to, and including, 3.3.19 via deserialization of untrusted input from the 'go_pricing' shortcode 'data' parameter. This allows authenticated attackers, with subscriber-level permissions and above, to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code. **CVE ID : CVE-2023-2500**		
N/A	24-May-2023	7.5	The Go Pricing - WordPress Responsive Pricing Tables plugin for WordPress is vulnerable to unauthorized arbitrary file uploads due to an improper capability check on the 'validate_upload' function in versions	N/A	A-GRA-GO_P-020623/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			up to, and including, 3.3.19. This makes it possible for authenticated attackers with a role that the administrator previously granted access to the plugin to upload arbitrary files on the affected site's server which may make remote code execution possible. **CVE ID : CVE-2023-2496**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	The Go Pricing - WordPress Responsive Pricing Tables plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 3.3.19 due to insufficient input sanitization and output escaping. This makes it possible for contributor-level attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	N/A	A-GRA-GO_P-020623/227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2498		
Vendor: groundhogg					
Product: groundhogg					
Affected Version(s): * Up to (including) 2.7.9.8					
Cross-Site Request Forgery (CSRF)	20-May-2023	8	The Groundhogg plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.7.9.8. This is due to missing nonce validation in the 'ajax_edit_contact' function. This makes it possible for authenticated attackers to receive the auto login link via shortcode and then modify the assigned user to the auto login link to elevate verified user privileges via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2736**	N/A	A-GRO-GROU-020623/228
Missing Authorization	20-May-2023	5.4	The Groundhogg plugin for WordPress is vulnerable to unauthorized	N/A	A-GRO-GROU-020623/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access of data and modification of data due to a missing capability check on the 'ajax_upload_file' function in versions up to, and including, 2.7.9.8. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload a file to the contact, and then lists all the other uploaded files related to the contact. **CVE ID : CVE-2023-2716**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-May-2023	5.4	The Groundhogg plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'gh_form' shortcode in versions up to, and including, 2.7.9.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above	N/A	A-GRO-GROU-020623/230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Please note this only works with legacy contact forms. **CVE ID : CVE-2023-2735**		
Missing Authorization	20-May-2023	4.3	The Groundhogg plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'check_license' functions in versions up to, and including, 2.7.9.8. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to change the license key and support license key, but it can only be changed to a valid license key. **CVE ID : CVE-2023-2714**	N/A	A-GRO-GROU-020623/231
Missing Authorization	20-May-2023	4.3	The Groundhogg plugin for WordPress is vulnerable to	N/A	A-GRO-GROU-020623/232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized modification of data due to a missing capability check on the 'submit_ticket' function in versions up to, and including, 2.7.9.8. This makes it possible for authenticated attackers to create a support ticket that sends the website's data to the plugin developer, and it is also possible to create an admin access with an auto login link that is also sent to the plugin developer with the ticket. It only works if the plugin is activated with a valid license. **CVE ID : CVE-2023-2715**		
Cross-Site Request Forgery (CSRF)	20-May-2023	4.3	The Groundhogg plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.7.9.8. This is due to missing nonce validation on the 'enable_safe_mode' function. This	N/A	A-GRO-GROU-020623/233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			makes it possible for unauthenticated attackers to enable safe mode, which disables all other plugins, via a forged request if they can successfully trick an administrator into performing an action such as clicking on a link. A warning message about safe mode is displayed to the admin, which can be easily disabled. **CVE ID : CVE-2023-2717**		
Vendor: guest_management_system_project					
Product: guest_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	6.1	A vulnerability, which was classified as problematic, has been found in SourceCodester Guest Management System 1.0. Affected by this issue is some unknown functionality of the file dateTest.php of the component GET Parameter Handler. The manipulation of the argument name leads to cross site scripting. The attack may be	N/A	A-GUE-GUES-020623/234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229160. **CVE ID : CVE-2023-2740**		
Vendor: hazelcast					
Product: hazelcast					
Affected Version(s): * Up to (including) 5.0.4					
Insufficiently Protected Credentials	22-May-2023	4.3	In Hazelcast through 5.0.4, 5.1 through 5.1.6, and 5.2 through 5.2.3, configuration routines don't mask passwords in the member configuration properly. This allows Hazelcast Management Center users to view some of the secrets. **CVE ID : CVE-2023-33264**	https://github.com/hazelcast/hazelcast/pull/24266	A-HAZ-HAZE-020623/235
Affected Version(s): From (including) 5.1 Up to (including) 5.1.6					
Insufficiently Protected Credentials	22-May-2023	4.3	In Hazelcast through 5.0.4, 5.1 through 5.1.6, and 5.2 through 5.2.3, configuration routines don't mask passwords in the member configuration properly. This	https://github.com/hazelcast/hazelcast/pull/24266	A-HAZ-HAZE-020623/236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows Hazelcast Management Center users to view some of the secrets. **CVE ID : CVE-2023-33264**		
Affected Version(s): From (including) 5.2 Up to (including) 5.2.3					
Insufficiently Protected Credentials	22-May-2023	4.3	In Hazelcast through 5.0.4, 5.1 through 5.1.6, and 5.2 through 5.2.3, configuration routines don't mask passwords in the member configuration properly. This allows Hazelcast Management Center users to view some of the secrets. **CVE ID : CVE-2023-33264**	https://github.com/hazelcast/hazelcast/pull/24266	A-HAZ-HAZE-020623/237
Vendor: hcl					
Product: domino_appdev_pack					
Affected Version(s): * Up to (excluding) 1.0.16					
N/A	23-May-2023	5.3	The HCL Domino AppDev Pack IAM service is susceptible to a User Account Enumeration vulnerability. During a failed login attempt a difference in messages could allow an attacker to determine if the	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0105093	A-HCL-DOMI-020623/238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user is valid or not. The attacker could use this information to focus a brute force attack on valid users. **CVE ID : CVE-2023-28015**		
Vendor: Hitachi					
Product: ops_center_analyzer					
Affected Version(s): 10.9.1-00					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	6.1	Cross-site Scripting vulnerability in Hitachi Ops Center Analyzer (Hitachi Ops Center Analyzer detail view component) allows Reflected XSS.This issue affects Hitachi Ops Center Analyzer: from 10.9.1-00 before 10.9.2-00. **CVE ID : CVE-2023-30469**	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2023-115/index.html	A-HIT-OPS_-020623/239
Vendor: hmplugin					
Product: wordpress_books_gallery					
Affected Version(s): * Up to (excluding) 4.4.9					
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in HM Plugin WordPress Books Gallery	N/A	A-HMP-WORD-020623/240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			plugin <= 4.4.8 versions. **CVE ID : CVE-2023-23705**		
Vendor: huggingface					
Product: transformers					
Affected Version(s): * Up to (excluding) 4.30.0					
Insecure Temporary File	18-May-2023	4.7	Insecure Temporary File in GitHub repository huggingface/transformers prior to 4.30.0. **CVE ID : CVE-2023-2800**	https://github.com/huggingface/transformers/commit/80ca92470938bbcc348e2d9cf4734c7c25cb1c43, https://huntr.dev/bounties/a3867b4e-6701-4418-8c20-3c6e7084a44a	A-HUG-TRAN-020623/241
Vendor: hypr					
Product: hypr_server					
Affected Version(s): * Up to (excluding) 8.0					
Missing Authentication for Critical Function	23-May-2023	8.8	Missing Authentication for critical function vulnerability in HYPR Server allows Authentication Bypass when using Legacy APIs.This issue affects HYPR Server: before 8.0 (with enabled Legacy APIs)	https://www.hypr.com/security-advisories	A-HYP-HYPR-020623/242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1837		
Vendor: i13websolution					
Product: video_carousel_slider_with_lightbox					
Affected Version(s): * Up to (excluding) 1.0.23					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	6.1	The video carousel slider with lightbox plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the search_term parameter in versions up to, and including, 1.0.22 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-2710**	N/A	A-I13-VIDE-020623/243
Product: video_gallery					
Affected Version(s): * Up to (excluding) 1.0.11					
Improper Neutralization of Input During Web Page	16-May-2023	6.1	The Video Gallery plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the	N/A	A-I13-VIDE-020623/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			'search_term' parameter in versions up to, and including, 1.0.10 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. **CVE ID : CVE-2023-2708**		
Vendor: IBM					
Product: infosphere_information_server					
Affected Version(s): 11.7					
Deserialization of Untrusted Data	22-May-2023	9.8	IBM InfoSphere Information Server 11.7 is affected by a remote code execution vulnerability due to insecure deserialization in an RMI service. IBM X-Force ID: 255285. **CVE ID : CVE-2023-32336**	https://www.ibm.com/support/pages/node/6995879, https://exchange.xforce.ibmcloud.com/vulnerabilities/255285	A-IBM-INFO-020623/245
Cleartext Storage of Sensitive	19-May-2023	5.5	IBM InfoSphere Information Server 11.7 stores user credentials in plain clear text which can	https://exchange.xforce.ibmcloud.com/vulnerabilities/244373,	A-IBM-INFO-020623/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Information			be read by a local user. IBM X-Force ID: 244373. **CVE ID : CVE-2023-22878**	https://https://www.ibm.com/support/pages/node/6988155	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 251213. **CVE ID : CVE-2023-28529**	https://www.ibm.com/support/pages/node/6988675, https://https://exchange.xforce.ibmcloud.com/vulnerabilities/251213	A-IBM-INFO-020623/247
Product: mq					
Affected Version(s): 8.0.0.0					
Generation of Error Message Containing Sensitive Information	19-May-2023	5.5	IBM MQ 8.0, 9.0, and 9.1 could allow a local user to obtain sensitive credential information when a detailed technical error message is returned in a stack trace. IBM X-Force ID: 250398. **CVE ID : CVE-2023-28514**	https://www.ibm.com/support/pages/node/6985835, https://exchange.xforce.ibmcloud.com/vulnerabilities/250398	A-IBM-MQ-020623/248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-May-2023	5.5	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose sensitive user information from a trace file if that functionality has been enabled. IBM X-Force ID: 251358. **CVE ID : CVE-2023-28950**	https://exchange.xforce.ibmcloud.com/vulnerabilities/251358, https://https://www.ibm.com/support/pages/node/6985837	A-IBM-MQ-020623/249
Affected Version(s): 9.0.0.0					
Generation of Error Message Containing Sensitive Information	19-May-2023	5.5	IBM MQ 8.0, 9.0, and 9.1 could allow a local user to obtain sensitive credential information when a detailed technical error message is returned in a stack trace. IBM X-Force ID: 250398. **CVE ID : CVE-2023-28514**	https://www.ibm.com/support/pages/node/6985835, https://exchange.xforce.ibmcloud.com/vulnerabilities/250398	A-IBM-MQ-020623/250
N/A	19-May-2023	5.5	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose sensitive user information from a trace file if that functionality has been enabled. IBM X-Force ID: 251358. **CVE ID : CVE-2023-28950**	https://exchange.xforce.ibmcloud.com/vulnerabilities/251358, https://https://www.ibm.com/support/pages/node/6985837	A-IBM-MQ-020623/251
Affected Version(s): 9.1.0					
Generation of Error	19-May-2023	5.5	IBM MQ 8.0, 9.0, and 9.1 could allow	https://www.ibm.com/supp	A-IBM-MQ-020623/252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Message Containing Sensitive Information			a local user to obtain sensitive credential information when a detailed technical error message is returned in a stack trace. IBM X-Force ID: 250398. **CVE ID : CVE-2023-28514**	ort/pages/node/6985835, https://exchange.xforce.ibmcloud.com/vulnerabilities/250398	
Affected Version(s): 9.1.0.0					
Generation of Error Message Containing Sensitive Information	19-May-2023	5.5	IBM MQ 8.0, 9.0, and 9.1 could allow a local user to obtain sensitive credential information when a detailed technical error message is returned in a stack trace. IBM X-Force ID: 250398. **CVE ID : CVE-2023-28514**	https://www.ibm.com/support/pages/node/6985835, https://exchange.xforce.ibmcloud.com/vulnerabilities/250398	A-IBM-MQ-020623/253
N/A	19-May-2023	5.5	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose sensitive user information from a trace file if that functionality has been enabled. IBM X-Force ID: 251358. **CVE ID : CVE-2023-28950**	https://exchange.xforce.ibmcloud.com/vulnerabilities/251358, https://https://www.ibm.com/support/pages/node/6985837	A-IBM-MQ-020623/254
Affected Version(s): 9.2.0					
N/A	19-May-2023	5.5	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose	https://exchange.xforce.ibmcloud.com/vul	A-IBM-MQ-020623/255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive user information from a trace file if that functionality has been enabled. IBM X-Force ID: 251358. **CVE ID : CVE-2023-28950**	nerabilities/251358, https://https://www.ibm.com/support/pages/node/6985837	
Affected Version(s): 9.3.0					
N/A	19-May-2023	5.5	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose sensitive user information from a trace file if that functionality has been enabled. IBM X-Force ID: 251358. **CVE ID : CVE-2023-28950**	https://exchange.xforce.ibmcloud.com/vulnerabilities/251358, https://https://www.ibm.com/support/pages/node/6985837	A-IBM-MQ-020623/256
Vendor: icecms_project					
Product: icecms					
Affected Version(s): 1.0.0					
N/A	25-May-2023	7.5	IceCMS v1.0.0 has Insecure Permissions. There is unauthorized access to the API, resulting in the disclosure of sensitive information. **CVE ID : CVE-2023-33355**	N/A	A-ICE-ICEC-020623/257
Improper Neutralization of Input During	25-May-2023	5.4	IceCMS v1.0.0 is vulnerable to Cross Site Scripting (XSS).	N/A	A-ICE-ICEC-020623/258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2023-33356**		
Vendor: idurar_project					
Product: idurar					
Affected Version(s): 1.0.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-May-2023	9.8	IDURAR ERP/CRM v1 was discovered to contain a SQL injection vulnerability via the component /api/login. **CVE ID : CVE-2023-27742**	N/A	A-IDU-IDUR-020623/259
Vendor: inkthemes					
Product: colorway					
Affected Version(s): * Up to (including) 4.2.3					
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Inkthemescom ColorWay theme <= 4.2.3 versions. **CVE ID : CVE-2023-25447**	N/A	A-INK-COLO-020623/260
Vendor: inspireui					
Product: mstore_api					
Affected Version(s): * Up to (including) 3.9.0					
N/A	25-May-2023	9.8	The MStore API plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.9.0.	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2913397%40mstore-	A-INS-MSTO-020623/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This is due to insufficient verification on the user being supplied during the coupon redemption REST API request through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the user id. **CVE ID : CVE-2023-2733**	api&old=2910707%40mstore-api&sfp_email=&sfph_mail=#file60, https://plugins.trac.wordpress.org/browser/mstore-api/tags/3.9.0/controllers/flutter-woo.php#L734	
Affected Version(s): * Up to (including) 3.9.1					
N/A	25-May-2023	9.8	The MStore API plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.9.1. This is due to insufficient verification on the user being supplied during the cart sync from mobile REST API request through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if	https://plugins.trac.wordpress.org/browser/mstore-api/tags/3.9.0/controllers/flutter-woo.php#L911, https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2915729%40mstore-api&old=2913397%40mstore-api&sfp_email=&sfph_mail=#file59	A-INS-MSTO-020623/262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they have access to the user id. **CVE ID : CVE-2023-2734**		
Affected Version(s): * Up to (including) 3.9.2					
N/A	25-May-2023	9.8	The MStore API plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.9.2. This is due to insufficient verification on the user being supplied during the add listing REST API request through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the user id. **CVE ID : CVE-2023-2732**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2916124%40mstore-api&old=2915729%40mstore-api&sfp_email=&sfph_mail=#file58	A-INS-MSTO-020623/263
Vendor: ipekyolunet					
Product: software_auto_damage_tracking_software					
Affected Version(s): * Up to (excluding) 4					
Improper Neutralization of Special Elements used in an SQL	24-May-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in	N/A	A-IPE-SOFT-020623/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			Ipekyolu Software Auto Damage Tracking Software allows SQL Injection.This issue affects Auto Damage Tracking Software: before 4. **CVE ID : CVE-2023-2045**		
Vendor: Jenkins					
Product: ansible					
Affected Version(s): * Up to (including) 204.v8191fd551eb_f					
Cleartext Storage of Sensitive Information	16-May-2023	5.3	Jenkins Ansible Plugin 204.v8191fd551eb_f and earlier does not mask extra variables displayed on the configuration form, increasing the potential for attackers to observe and capture them. **CVE ID : CVE-2023-32983**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3017	A-JEN-ANSI-020623/265
Missing Encryption of Sensitive Data	16-May-2023	4.3	Jenkins Ansible Plugin 204.v8191fd551eb_f and earlier stores extra variables unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3017	A-JEN-ANSI-020623/266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Item/Extended Read permission or access to the Jenkins controller file system. **CVE ID : CVE-2023-32982**		
Product: appspider					
Affected Version(s): * Up to (including) 1.0.15					
Cross-Site Request Forgery (CSRF)	16-May-2023	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins AppSpider Plugin 1.0.15 and earlier allows attackers to connect to an attacker-specified URL and send an HTTP POST request with a JSON payload consisting of attacker-specified credentials. **CVE ID : CVE-2023-32998**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3121	A-JEN-APPS-020623/267
Incorrect Default Permissions	16-May-2023	4.3	A missing permission check in Jenkins AppSpider Plugin 1.0.15 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL and send an HTTP POST request with a JSON payload consisting of attacker-	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3121	A-JEN-APPS-020623/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified credentials. **CVE ID : CVE-2023-32999**		
Product: azure_vm_agents					
Affected Version(s): * Up to (including) 852.v8d35f0960a_43					
Cross-Site Request Forgery (CSRF)	16-May-2023	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins Azure VM Agents Plugin 852.v8d35f0960a_43 and earlier allows attackers to connect to an attacker-specified Azure Cloud server using attacker-specified credentials IDs obtained through another method. **CVE ID : CVE-2023-32989**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2855%20(2)	A-JEN-AZUR-020623/269
Incorrect Permission Assignment for Critical Resource	16-May-2023	6.5	A missing permission check in Jenkins Azure VM Agents Plugin 852.v8d35f0960a_43 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified Azure Cloud server using attacker-specified credentials IDs obtained through another method.	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2855%20(2)	A-JEN-AZUR-020623/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32990		
Insufficiently Protected Credentials	16-May-2023	4.3	A missing permission check in Jenkins Azure VM Agents Plugin 852.v8d35f0960a_43 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. **CVE ID : CVE-2023-32988**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2855%20(1)	A-JEN-AZUR-020623/271
Product: cas					
Affected Version(s): * Up to (including) 1.6.2					
Session Fixation	16-May-2023	8.8	Jenkins CAS Plugin 1.6.2 and earlier does not invalidate the previous session on login. **CVE ID : CVE-2023-32997**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3000	A-JEN-CAS-020623/272
Product: code_dx					
Affected Version(s): * Up to (including) 3.1.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-May-2023	4.3	A missing permission check in Jenkins Code Dx Plugin 3.1.0 and earlier allows attackers with Item/Read permission to check for the existence of an attacker-specified file path on an agent file system.	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3145	A-JEN-CODE-020623/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2196		
Cross-Site Request Forgery (CSRF)	16-May-2023	4.3	A missing permission check in Jenkins Code Dx Plugin 3.1.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL. **CVE ID : CVE-2023-2631**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3118	A-JEN-CODE-020623/274
Insufficiently Protected Credentials	16-May-2023	4.3	Jenkins Code Dx Plugin 3.1.0 and earlier stores Code Dx server API keys unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system. **CVE ID : CVE-2023-2632**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3146	A-JEN-CODE-020623/275
Insufficiently Protected Credentials	16-May-2023	4.3	Jenkins Code Dx Plugin 3.1.0 and earlier does not mask Code Dx server API keys displayed on the configuration form, increasing the potential for attackers to	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3146	A-JEN-CODE-020623/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			observe and capture them. **CVE ID : CVE-2023-2633**		
Cross-Site Request Forgery (CSRF)	16-May-2023	3.5	A cross-site request forgery (CSRF) vulnerability in Jenkins Code Dx Plugin 3.1.0 and earlier allows attackers to connect to an attacker-specified URL. **CVE ID : CVE-2023-2195**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3118	A-JEN-CODE-020623/277
Product: email_extension					
Affected Version(s): * Up to (including) 2.96					
Incorrect Permission Assignment for Critical Resource	16-May-2023	4.3	Jenkins Email Extension Plugin does not perform a permission check in a method implementing form validation, allowing attackers with Overall/Read permission to check for the existence of files in the email-templates/ directory in the Jenkins home directory on the controller file system. **CVE ID : CVE-2023-32979**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3088%20(1)	A-JEN-EMAI-020623/278
Cross-Site Request	16-May-2023	4.3	A cross-site request forgery (CSRF) vulnerability in	https://www.jenkins.io/security/advisory/	A-JEN-EMAI-020623/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Jenkins Email Extension Plugin allows attackers to make another user stop watching an attacker-specified job. **CVE ID : CVE-2023-32980**	2023-05-16/#SECURITY-3088%20(2)	
Product: file_parameters					
Affected Version(s): * Up to (including) 285.287.v4b_7b_29d3469d					
Incorrect Permission Assignment for Critical Resource	16-May-2023	8.8	Jenkins File Parameter Plugin 285.v757c5b_67a_c25 and earlier does not restrict the name (and resulting uploaded file name) of Stashed File Parameters, allowing attackers with Item/Configure permission to create or replace arbitrary files on the Jenkins controller file system with attacker-specified content. **CVE ID : CVE-2023-32986**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3123	A-JEN-FILE-020623/280
Product: hashicorp_vault					
Affected Version(s): * Up to (including) 360.v0a_1c04cf807d					
Insertion of Sensitive Information into Log File	16-May-2023	7.5	Jenkins HashiCorp Vault Plugin 360.v0a_1c04cf807d and earlier does not properly mask	https://www.jenkins.io/security/advisory/2023-05-	A-JEN-HASH-020623/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(i.e., replace with asterisks) credentials in the build log when push mode for durable task logging is enabled. **CVE ID : CVE-2023-33001**	16/#SECURITY-3077	
Product: lightweight_directory_access_protocol					
Affected Version(s): * Up to (excluding) 673.v034ec70ec2b_b					
Cross-Site Request Forgery (CSRF)	16-May-2023	4.3	A cross-site request forgery (CSRF) vulnerability in Jenkins LDAP Plugin allows attackers to connect to an attacker-specified LDAP server using attacker-specified credentials. **CVE ID : CVE-2023-32978**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3046	A-JEN-LIGH-020623/282
Product: loadcomplete_support					
Affected Version(s): * Up to (including) 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	5.4	Jenkins LoadComplete support Plugin 1.0 and earlier does not escape the LoadComplete test name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2903	A-JEN-LOAD-020623/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33007		
Product: ns-nd_integration_performance_publisher					
Affected Version(s): * Up to (including) 4.8.0.149					
Insufficiently Protected Credentials	16-May-2023	7.5	Jenkins NS-ND Integration Performance Publisher Plugin 4.8.0.149 and earlier does not mask credentials displayed on the configuration form, increasing the potential for attackers to observe and capture them. **CVE ID : CVE-2023-33000**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2962	A-JEN-NS-N-020623/284
Product: pipeline					
Affected Version(s): _job Up to (including) 1292.v27d8cc3e2602					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	5.4	Jenkins Pipeline: Job Plugin does not escape the display name of the build that caused an earlier build to be aborted, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to set build display names immediately. **CVE ID : CVE-2023-32977**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3042	A-JEN-PIPE-020623/285
Product: pipeline_utility_steps					
Affected Version(s): * Up to (including) 2.15.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-May-2023	9.8	An arbitrary file write vulnerability in Jenkins Pipeline Utility Steps Plugin 2.15.2 and earlier allows attackers able to provide crafted archives as parameters to create or replace arbitrary files on the agent file system with attacker-specified content. **CVE ID : CVE-2023-32981**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2196	A-JEN-PIPE-020623/286
Product: reverse_proxy_auth					
Affected Version(s): * Up to (including) 1.7.4					
Cross-Site Request Forgery (CSRF)	16-May-2023	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins Reverse Proxy Auth Plugin 1.7.4 and earlier allows attackers to connect to an attacker-specified LDAP server using attacker-specified credentials. **CVE ID : CVE-2023-32987**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3002	A-JEN-REVE-020623/287
Product: saml_single_sign-on					
Affected Version(s): * Up to (including) 2.0.0					
Incorrect Default Permissions	16-May-2023	4.3	A missing permission check in Jenkins SAML Single Sign On(SSO) Plugin 2.0.0 and earlier allows	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2994	A-JEN-SAML-020623/288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers with Overall/Read permission to send an HTTP POST request with JSON body containing attacker-specified content, to miniOrange's API for sending emails. **CVE ID : CVE-2023-32996**		
Product: saml_single_sign_on					
Affected Version(s): * Up to (including) 2.0.0					
Cross-Site Request Forgery (CSRF)	16-May-2023	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins SAML Single Sign On(SSO) Plugin 2.0.0 and earlier allows attackers to send an HTTP POST request with JSON body containing attacker-specified content, to miniOrange's API for sending emails. **CVE ID : CVE-2023-32995**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2994	A-JEN-SAML-020623/289
Affected Version(s): * Up to (including) 2.0.2					
Cross-Site Request Forgery (CSRF)	16-May-2023	8.8	A cross-site request forgery (CSRF) vulnerability in Jenkins SAML Single Sign On(SSO) Plugin 2.0.2 and earlier allows attackers to send an HTTP request to an attacker-	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2993	A-JEN-SAML-020623/290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified URL and parse the response as XML, or parse a local file on the Jenkins controller as XML. **CVE ID : CVE-2023-32991**		
Incorrect Permission Assignment for Critical Resource	16-May-2023	8.8	Missing permission checks in Jenkins SAML Single Sign On(SSO) Plugin 2.0.2 and earlier allow attackers with Overall/Read permission to send an HTTP request to an attacker-specified URL and parse the response as XML, or parse a local file on the Jenkins controller as XML. **CVE ID : CVE-2023-32992**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2993	A-JEN-SAML-020623/291
Insufficient Verification of Data Authenticity	16-May-2023	4.8	Jenkins SAML Single Sign On(SSO) Plugin 2.0.2 and earlier does not perform hostname validation when connecting to miniOrange or the configured IdP to retrieve SAML metadata, which could be abused using a man-in-the-middle attack to intercept these connections.	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3001%20(1)	A-JEN-SAML-020623/292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32993		
Affected Version(s): * Up to (including) 2.1.0					
Improper Certificate Validation	16-May-2023	3.7	Jenkins SAML Single Sign On(SSO) Plugin 2.1.0 and earlier unconditionally disables SSL/TLS certificate validation for connections to miniOrange or the configured IdP to retrieve SAML metadata, which could be abused using a man-in-the-middle attack to intercept these connections. **CVE ID : CVE-2023-32994**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3001%20(2)	A-JEN-SAML-020623/293
Product: sidebar_link					
Affected Version(s): * Up to (including) 2.2.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-May-2023	4.3	Jenkins Sidebar Link Plugin 2.2.1 and earlier does not restrict the path of files in a method implementing form validation, allowing attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3125	A-JEN-SIDE-020623/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32985		
Product: tag_profiler					
Affected Version(s): * Up to (including) 0.2					
Cross-Site Request Forgery (CSRF)	16-May-2023	4.3	A cross-site request forgery (CSRF) vulnerability in Jenkins Tag Profiler Plugin 0.2 and earlier allows attackers to reset profiler statistics. **CVE ID : CVE-2023-33003**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3083	A-JEN-TAG_-020623/295
Incorrect Permission Assignment for Critical Resource	16-May-2023	4.3	A missing permission check in Jenkins Tag Profiler Plugin 0.2 and earlier allows attackers with Overall/Read permission to reset profiler statistics. **CVE ID : CVE-2023-33004**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3083	A-JEN-TAG_-020623/296
Product: testcomplete_support					
Affected Version(s): * Up to (including) 2.8.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	5.4	Jenkins TestComplete support Plugin 2.8.1 and earlier does not escape the TestComplete project name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2892	A-JEN-TEST-020623/297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Item/Configure permission. **CVE ID : CVE-2023-33002**		
Product: testng_results					
Affected Version(s): * Up to (including) 730.v4c5283037693					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	5.4	Jenkins TestNG Results Plugin 730.v4c5283037693 and earlier does not escape several values that are parsed from TestNG report files and displayed on the plugin's test information pages, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide a crafted TestNG report file. **CVE ID : CVE-2023-32984**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-3047	A-JEN-TEST-020623/298
Product: wso2_oauth					
Affected Version(s): * Up to (including) 1.0					
Insufficient Session Expiration	16-May-2023	5.4	Jenkins WSO2 Oauth Plugin 1.0 and earlier does not invalidate the previous session on login. **CVE ID : CVE-2023-33005**	https://www.jenkins.io/security/advisory/2023-05-16/#SECURITY-2991	A-JEN-WSO2-020623/299
Cross-Site Request	16-May-2023	5.4	A cross-site request forgery (CSRF) vulnerability in Jenkins WSO2	https://www.jenkins.io/security/advisory/2023-05-	A-JEN-WSO2-020623/300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Oauth Plugin 1.0 and earlier allows attackers to trick users into logging in to the attacker's account. **CVE ID : CVE-2023-33006**	16/#SECURITY-2990	
Vendor: jizhicms					
Product: jizhicms					
Affected Version(s): 2.4.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-2023	5.4	jizhicms v2.4.6 is vulnerable to Cross Site Scripting (XSS). The content of the article published in the front end is only filtered in the front end, without being filtered in the background, which allows attackers to publish an article containing malicious JavaScript scripts by modifying the request package. **CVE ID : CVE-2023-31862**	N/A	A-JIZ-JIZH-020623/301
Vendor: Kubernetes					
Product: minikube					
Affected Version(s): 1.26.0					
N/A	24-May-2023	9.8	This vulnerability exposes a network port in minikube running on macOS with Docker driver that could enable unexpected remote access to the	N/A	A-KUB-MINI-020623/302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			minikube container. **CVE ID : CVE-2023-1174**		
Affected Version(s): 1.26.1					
N/A	24-May-2023	9.8	This vulnerability exposes a network port in minikube running on macOS with Docker driver that could enable unexpected remote access to the minikube container. **CVE ID : CVE-2023-1174**	N/A	A-KUB-MINI-020623/303
Affected Version(s): 1.27.0					
N/A	24-May-2023	9.8	This vulnerability exposes a network port in minikube running on macOS with Docker driver that could enable unexpected remote access to the minikube container. **CVE ID : CVE-2023-1174**	N/A	A-KUB-MINI-020623/304
Affected Version(s): 1.27.1					
N/A	24-May-2023	9.8	This vulnerability exposes a network port in minikube running on macOS with Docker driver that could enable unexpected remote access to the minikube container.	N/A	A-KUB-MINI-020623/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1174		
Affected Version(s): 1.28.0					
N/A	24-May-2023	9.8	This vulnerability exposes a network port in minikube running on macOS with Docker driver that could enable unexpected remote access to the minikube container. **CVE ID : CVE-2023-1174**	N/A	A-KUB-MINI-020623/306
Vendor: lavalite					
Product: lavalite					
Affected Version(s): 9.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-May-2023	5.4	LavaLite v9.0.0 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-30124**	N/A	A-LAV-LAVA-020623/307
Vendor: lfprojects					
Product: mlflow					
Affected Version(s): * Up to (excluding) 2.3.1					
Path Traversal: '..filename'	17-May-2023	9.8	Path Traversal: '\..\filename' in GitHub repository mlflow/mlflow prior to 2.3.1. **CVE ID : CVE-2023-2780**	https://huntr.dev/bounties/b12b0073-0bb0-4bd1-8fc2-ec7f17fd7689, https://github.com/mlflow/mlflow/commit/fae77a525d	A-LFP-MLFL-020623/308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				d908c56d6204a4cef1c1c75b4e9857	
Vendor: Libreswan					
Product: libreswan					
Affected Version(s): 4.9-1.el8					
N/A	17-May-2023	7.5	A vulnerability was found in the libreswan library. This security issue occurs when an IKEv1 Aggressive Mode packet is received with only unacceptable crypto algorithms, and the response packet is not sent with a zero responder SPI. When a subsequent packet is received where the sender reuses the libreswan responder SPI as its own initiator SPI, the pluto daemon state machine crashes. No remote code execution is possible. This CVE exists because of a CVE-2023-30570 security regression for libreswan package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2.	N/A	A-LIB-LIBR-020623/309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2295		
Affected Version(s): 4.9-1.el9					
N/A	17-May-2023	7.5	A vulnerability was found in the libreswan library. This security issue occurs when an IKEv1 Aggressive Mode packet is received with only unacceptable crypto algorithms, and the response packet is not sent with a zero responder SPI. When a subsequent packet is received where the sender reuses the libreswan responder SPI as its own initiator SPI, the pluto daemon state machine crashes. No remote code execution is possible. This CVE exists because of a CVE-2023-30570 security regression for libreswan package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2295**	N/A	A-LIB-LIBR-020623/310
Vendor: Libtiff					
Product: libtiff					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 4.0.0					
Out-of-bounds Write	19-May-2023	5.5	A vulnerability was found in the libtiff library. This flaw causes a heap buffer overflow issue via the TIFFTAG_INKNAMES and TIFFTAG_NUMBEROFINKS values. **CVE ID : CVE-2023-30774**	N/A	A-LIB-LIBT-020623/311
Affected Version(s): * Up to (excluding) 4.5.0					
NULL Pointer Dereference	17-May-2023	5.5	A NULL pointer dereference flaw was found in Libtiff's LZWDecode() function in the libtiff/tif_lzw.c file. This flaw allows a local attacker to craft specific input data that can cause the program to dereference a NULL pointer when decompressing a TIFF format file, resulting in a program crash or denial of service. **CVE ID : CVE-2023-2731**	https://github.com/libsdl-org/libtiff/commit/9be22b639ea69e102d3847dca4c53ef025e9527b, https://bugzilla.redhat.com/show_bug.cgi?id=2207635, https://gitlab.com/libtiff/libtiff/-/issues/548	A-LIB-LIBT-020623/312
Affected Version(s): 4.4.0					
Out-of-bounds Write	19-May-2023	5.5	A vulnerability was found in the libtiff library. This security flaw causes a heap buffer overflow in	https://gitlab.com/libtiff/libtiff/-/issues/464	A-LIB-LIBT-020623/313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			extractContigSamples32bits, tiffcrop.c. **CVE ID : CVE-2023-30775**		
Vendor: Liferay					
Product: digital_experience_platform					
Affected Version(s): 7.0					
Insecure Default Initialization of Resource	24-May-2023	7.5	In Liferay Portal 7.3.0 and earlier, and Liferay DXP 7.2 and earlier the default configuration does not require users to verify their email address, which allows remote attackers to create accounts using fake email addresses or email addresses which they don't control. The portal property `company.security.strangers.verify` should be set to true. **CVE ID : CVE-2023-33949**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33949	A-LIF-DIGI-020623/314
Affected Version(s): 7.1					
Insecure Default Initialization of Resource	24-May-2023	7.5	In Liferay Portal 7.3.0 and earlier, and Liferay DXP 7.2 and earlier the default configuration does not require users to verify their email address, which allows remote	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33949	A-LIF-DIGI-020623/315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to create accounts using fake email addresses or email addresses which they don't control. The portal property `company.security.strangers.verify` should be set to true. **CVE ID : CVE-2023-33949**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Stored cross-site scripting (XSS) vulnerability in Form widget configuration in Liferay Portal 7.1.0 through 7.3.0, and Liferay DXP 7.1 before fix pack 18, and 7.2 before fix pack 5 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a form's `name` field. **CVE ID : CVE-2023-33937**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33937	A-LIF-DIGI-020623/316
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Cross-site scripting (XSS) vulnerability in the Modified Facet widget in Liferay Portal 7.1.0 through 7.4.3.12, and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 18, 7.3 before update 4, and 7.4	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33939	A-LIF-DIGI-020623/317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before update 9 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a facet label. **CVE ID : CVE-2023-33939**		
Affected Version(s): 7.2					
Insecure Default Initialization of Resource	24-May-2023	7.5	In Liferay Portal 7.3.0 and earlier, and Liferay DXP 7.2 and earlier the default configuration does not require users to verify their email address, which allows remote attackers to create accounts using fake email addresses or email addresses which they don't control. The portal property `company.security.strangers.verify` should be set to true. **CVE ID : CVE-2023-33949**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33949	A-LIF-DIGI-020623/318
Improper Neutralization of Input During Web Page Generation	24-May-2023	5.4	Stored cross-site scripting (XSS) vulnerability in Form widget configuration in Liferay Portal 7.1.0 through 7.3.0, and Liferay DXP 7.1	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/conte	A-LIF-DIGI-020623/319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			before fix pack 18, and 7.2 before fix pack 5 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a form's `name` field. **CVE ID : CVE-2023-33937**	nt/cve-2023-33937	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Cross-site scripting (XSS) vulnerability in the Modified Facet widget in Liferay Portal 7.1.0 through 7.4.3.12, and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 18, 7.3 before update 4, and 7.4 before update 9 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a facet label. **CVE ID : CVE-2023-33939**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33939	A-LIF-DIGI-020623/320
Affected Version(s): 7.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	6.1	Cross-site scripting (XSS) vulnerability in the App Builder module's custom object details page in Liferay Portal 7.3.0 through 7.4.0, and Liferay DXP 7.3 before update 14	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/conte	A-LIF-DIGI-020623/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an App Builder custom object's `Name` field. **CVE ID : CVE-2023-33938**	nt/cve-2023-33938	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Cross-site scripting (XSS) vulnerability in the Modified Facet widget in Liferay Portal 7.1.0 through 7.4.3.12, and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 18, 7.3 before update 4, and 7.4 before update 9 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a facet label. **CVE ID : CVE-2023-33939**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33939	A-LIF-DIGI-020623/322
Affected Version(s): 7.4					
N/A	24-May-2023	7.5	Pattern Redirects in Liferay Portal 7.4.3.48 through 7.4.3.76, and Liferay DXP 7.4 update 48 through 76 allows regular expressions that are vulnerable to	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/conte	A-LIF-DIGI-020623/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ReDoS attacks to be used as patterns, which allows remote attackers to consume an excessive amount of server resources via crafted request URLs. **CVE ID : CVE-2023-33950**	nt/cve-2023-33950	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	6.1	Multiple cross-site scripting (XSS) vulnerabilities in the Plugin for OAuth 2.0 module's OAuth2ProviderApplicationRedirect class in Liferay Portal 7.4.3.41 through 7.4.3.52, and Liferay DXP 7.4 update 41 through 52 allow remote attackers to inject arbitrary web script or HTML via the (1) code, or (2) error parameter. **CVE ID : CVE-2023-33941**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33941	A-LIF-DIGI-020623/324
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Cross-site scripting (XSS) vulnerability in the Modified Facet widget in Liferay Portal 7.1.0 through 7.4.3.12, and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 18, 7.3 before update 4, and 7.4 before update 9	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33939	A-LIF-DIGI-020623/325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a facet label. **CVE ID : CVE-2023-33939**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Cross-site scripting (XSS) vulnerability in IFrame type Remote Apps in Liferay Portal 7.4.0 through 7.4.3.30, and Liferay DXP 7.4 before update 31 allows remote attackers to inject arbitrary web script or HTML via the Remote App's IFrame URL. **CVE ID : CVE-2023-33940**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33940	A-LIF-DIGI-020623/326
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Cross-site scripting (XSS) vulnerability in the Web Content Display widget's article selector in Liferay Liferay Portal 7.4.3.50, and Liferay DXP 7.4 update 50 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a web content article's `Title` field.	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33942	A-LIF-DIGI-020623/327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33942		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Cross-site scripting (XSS) vulnerability in the Account module in Liferay Portal 7.4.3.21 through 7.4.3.62, and Liferay DXP 7.4 update 21 through 62 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a user's (1) First Name, (2) Middle Name, (3) Last Name, or (4) Job Title text field. **CVE ID : CVE-2023-33943**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33943	A-LIF-DIGI-020623/328
Product: liferay_portal					
Affected Version(s): 7.4.3.50					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Cross-site scripting (XSS) vulnerability in the Web Content Display widget's article selector in Liferay Liferay Portal 7.4.3.50, and Liferay DXP 7.4 update 50 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a web content article's `Title` field.	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33942	A-LIF-LIFE-020623/329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33942		
Affected Version(s): From (including) 7.0.0 Up to (including) 7.3.0					
Insecure Default Initialization of Resource	24-May-2023	7.5	In Liferay Portal 7.3.0 and earlier, and Liferay DXP 7.2 and earlier the default configuration does not require users to verify their email address, which allows remote attackers to create accounts using fake email addresses or email addresses which they don't control. The portal property `company.security.strangers.verify` should be set to true. **CVE ID : CVE-2023-33949**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33949	A-LIF-LIFE-020623/330
Affected Version(s): From (including) 7.1.0 Up to (excluding) 7.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Stored cross-site scripting (XSS) vulnerability in Form widget configuration in Liferay Portal 7.1.0 through 7.3.0, and Liferay DXP 7.1 before fix pack 18, and 7.2 before fix pack 5 allows remote attackers to inject arbitrary web script or HTML via a crafted payload	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33937	A-LIF-LIFE-020623/331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected into a form's `name` field. **CVE ID : CVE-2023-33937**		
Affected Version(s): From (including) 7.1.0 Up to (including) 7.4.3.12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Cross-site scripting (XSS) vulnerability in the Modified Facet widget in Liferay Portal 7.1.0 through 7.4.3.12, and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 18, 7.3 before update 4, and 7.4 before update 9 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a facet label. **CVE ID : CVE-2023-33939**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33939	A-LIF-LIFE-020623/332
Affected Version(s): From (including) 7.3.0 Up to (including) 7.4.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	6.1	Cross-site scripting (XSS) vulnerability in the App Builder module's custom object details page in Liferay Portal 7.3.0 through 7.4.0, and Liferay DXP 7.3 before update 14 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33938	A-LIF-LIFE-020623/333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			App Builder custom object's `Name` field. **CVE ID : CVE-2023-33938**		
Affected Version(s): From (including) 7.4.0 Up to (including) 7.4.3.30					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Cross-site scripting (XSS) vulnerability in IFrame type Remote Apps in Liferay Portal 7.4.0 through 7.4.3.30, and Liferay DXP 7.4 before update 31 allows remote attackers to inject arbitrary web script or HTML via the Remote App's IFrame URL. **CVE ID : CVE-2023-33940**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33940	A-LIF-LIFE-020623/334
Affected Version(s): From (including) 7.4.3.21 Up to (including) 7.4.3.62					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	Cross-site scripting (XSS) vulnerability in the Account module in Liferay Portal 7.4.3.21 through 7.4.3.62, and Liferay DXP 7.4 update 21 through 62 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a user's (1) First Name, (2) Middle Name, (3) Last Name, or (4) Job Title text field.	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33943	A-LIF-LIFE-020623/335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33943		
Affected Version(s): From (including) 7.4.3.31 Up to (including) 7.4.3.52					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	6.1	Multiple cross-site scripting (XSS) vulnerabilities in the Plugin for OAuth 2.0 module's OAuth2ProviderApplicationRedirect class in Liferay Portal 7.4.3.41 through 7.4.3.52, and Liferay DXP 7.4 update 41 through 52 allow remote attackers to inject arbitrary web script or HTML via the (1) code, or (2) error parameter. **CVE ID : CVE-2023-33941**	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33941	A-LIF-LIFE-020623/336
Affected Version(s): From (including) 7.4.3.48 Up to (including) 7.4.3.76					
N/A	24-May-2023	7.5	Pattern Redirects in Liferay Portal 7.4.3.48 through 7.4.3.76, and Liferay DXP 7.4 update 48 through 76 allows regular expressions that are vulnerable to ReDoS attacks to be used as patterns, which allows remote attackers to consume an excessive amount of server resources via crafted request URLs.	https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-33950	A-LIF-LIFE-020623/337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33950		
Vendor: lightbend					
Product: akka_http					
Affected Version(s): * Up to (excluding) 10.5.2					
N/A	21-May-2023	5.5	When Akka HTTP before 10.5.2 accepts file uploads via the FileUploadDirectives.fileUploadAll directive, the temporary file it creates has too weak permissions: it is readable by other users on Linux or UNIX, a similar issue to CVE-2022-41946. **CVE ID : CVE-2023-33251**	https://akka.io/security/akka-http-cve-2023-05-15.html	A-LIG-AKKA-020623/338
Vendor: Linuxfoundation					
Product: cups-filters					
Affected Version(s): * Up to (excluding) 2.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-May-2023	8.8	cups-filters contains backends, filters, and other software required to get the cups printing service working on operating systems other than macos. If you use the Backend Error Handler (beh) to create an accessible network printer, this security vulnerability can	https://github.com/OpenPrinting/cups-filters/security/advisories/GHSA-gpxc-v2m8-fr3x, https://github.com/OpenPrinting/cups-filters/commit/8f274035756c04efeb77eb654e9d4c4447287d65	A-LIN-CUPS-020623/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause remote code execution. `beh.c` contains the line `retval = system(cmdline) >> 8;` which calls the `system` command with the operand `cmdline`. `cmdline` contains multiple user controlled, unsanitized values. As a result an attacker with network access to the hosted print server can exploit this vulnerability to inject system commands which are executed in the context of the running server. This issue has been addressed in commit `8f2740357` and is expected to be bundled in the next release. Users are advised to upgrade when possible and to restrict access to network printers in the meantime. **CVE ID : CVE-2023-24805**		
Affected Version(s): 2.0					
Improper Neutralization of Special Elements	17-May-2023	8.8	cups-filters contains backends, filters, and other software required to get the cups	https://github.com/OpenPrinting/cups-filters/security/advisories/	A-LIN-CUPS-020623/340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			printing service working on operating systems other than macos. If you use the Backend Error Handler (beh) to create an accessible network printer, this security vulnerability can cause remote code execution. `beh.c` contains the line `retval = system(cmdline) >> 8;` which calls the `system` command with the operand `cmdline`. `cmdline` contains multiple user controlled, unsanitized values. As a result an attacker with network access to the hosted print server can exploit this vulnerability to inject system commands which are executed in the context of the running server. This issue has been addressed in commit `8f2740357` and is expected to be bundled in the next release. Users are advised to upgrade when possible and to restrict access to	GHSA-gpxc-v2m8-fr3x, https://github.com/OpenPrinting/cups-filters/commit/8f274035756c04efeb77eb654e9d4c4447287d65	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network printers in the meantime. **CVE ID : CVE-2023-24805**		
Vendor: ljapps					
Product: wp_airbnb_review_slider					
Affected Version(s): * Up to (including) 3.2					
Cross-Site Request Forgery (CSRF)	20-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in LJ Apps WP Airbnb Review Slider plugin <= 3.2 versions. **CVE ID : CVE-2023-23890**	N/A	A-LJA-WP_A-020623/341
Vendor: luatex_project					
Product: luatex					
Affected Version(s): From (including) 1.04 Up to (excluding) 1.16.2					
N/A	20-May-2023	7.8	LuaTeX before 1.17.0 allows execution of arbitrary shell commands when compiling a TeX file obtained from an untrusted source. This occurs because luatex-core.lua lets the original io.popen be accessed. This also affects TeX Live before 2023 r66984 and MiKTeX before 23.5. **CVE ID : CVE-2023-32700**	https://tug.org/~mseven/luatex.html	A-LUA-LUAT-020623/342
Vendor: luowice					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: luowice					
Affected Version(s): 3.5.18					
N/A	16-May-2023	7.5	Insecure permissions in luowice 3.5.18 allow attackers to view information for other alarm devices via modification of the eseeid parameter. **CVE ID : CVE-2023-31677**	N/A	A-LUO-LUOW-020623/343
Vendor: madewithfuel					
Product: better_notifications_for_wp					
Affected Version(s): * Up to (excluding) 1.9.3					
Cross-Site Request Forgery (CSRF)	26-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Made with Fuel Better Notifications for WP plugin <= 1.9.2 versions. **CVE ID : CVE-2023-32964**	N/A	A-MAD-BETT-020623/344
Vendor: metabase					
Product: metabase					
Affected Version(s): * Up to (excluding) 0.44.7					
Missing Authentication for Critical Function	18-May-2023	9.6	Metabase is an open source business analytics engine. To edit SQL Snippets, Metabase should have required people to be in at least one group with native query editing permissions to a database–but	https://github.com/metabase/metabase/pull/30852, https://github.com/metabase/metabase/security/advisories/GHSA-mw6j-f894-4qxv, https://github	A-MET-META-020623/345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			affected versions of Metabase didn't enforce that requirement. This lack of enforcement meant that: Anyone–including people in sandboxed groups–could edit SQL snippets. They could edit snippets via the API or, in the application UI, when editing the metadata for a model based on a SQL question, and people in sandboxed groups could edit a SQL snippet used in a query that creates their sandbox. If the snippet contained logic that restricted which data that person could see, they could potentially edit that snippet and change their level of data access. The permissions model for SQL snippets has been fixed in Metabase versions 0.46.3, 0.45.4, 0.44.7, 1.46.3, 1.45.4, and 1.44.7. Users are advised to upgrade. Users unable to upgrade should ensure that	.com/metabase/metabase/pull/30853, https://github.com/metabase/metabase/pull/30854	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SQL queries used to create sandboxes exclude SQL snippets. **CVE ID : CVE-2023-32680**		
Affected Version(s): From (including) 0.45.0 Up to (excluding) 0.45.4					
Missing Authentication for Critical Function	18-May-2023	9.6	Metabase is an open source business analytics engine. To edit SQL Snippets, Metabase should have required people to be in at least one group with native query editing permissions to a database–but affected versions of Metabase didn't enforce that requirement. This lack of enforcement meant that: Anyone–including people in sandboxed groups–could edit SQL snippets. They could edit snippets via the API or, in the application UI, when editing the metadata for a model based on a SQL question, and people in sandboxed groups could edit a SQL snippet used in a query that creates their sandbox. If the	https://github.com/metabase/metabase/pull/30852, https://github.com/metabase/metabase/security/advisories/GHSA-mw6j-f894-4qxv, https://github.com/metabase/metabase/pull/30853, https://github.com/metabase/metabase/pull/30854	A-MET-META-020623/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			snippet contained logic that restricted which data that person could see, they could potentially edit that snippet and change their level of data access. The permissions model for SQL snippets has been fixed in Metabase versions 0.46.3, 0.45.4, 0.44.7, 1.46.3, 1.45.4, and 1.44.7. Users are advised to upgrade. Users unable to upgrade should ensure that SQL queries used to create sandboxes exclude SQL snippets. **CVE ID : CVE-2023-32680**		
Affected Version(s): From (including) 0.46.0 Up to (excluding) 0.46.3					
Missing Authentication for Critical Function	18-May-2023	9.6	Metabase is an open source business analytics engine. To edit SQL Snippets, Metabase should have required people to be in at least one group with native query editing permissions to a database–but affected versions of Metabase didn't enforce that requirement. This	https://github.com/metabase/metabase/pull/30852, https://github.com/metabase/metabase/security/advisories/GHSA-mw6j-f894-4qxv, https://github.com/metabase/metabase/pull/30853, https://github	A-MET-META-020623/347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			lack of enforcement meant that: Anyone–including people in sandboxed groups–could edit SQL snippets. They could edit snippets via the API or, in the application UI, when editing the metadata for a model based on a SQL question, and people in sandboxed groups could edit a SQL snippet used in a query that creates their sandbox. If the snippet contained logic that restricted which data that person could see, they could potentially edit that snippet and change their level of data access. The permissions model for SQL snippets has been fixed in Metabase versions 0.46.3, 0.45.4, 0.44.7, 1.46.3, 1.45.4, and 1.44.7. Users are advised to upgrade. Users unable to upgrade should ensure that SQL queries used to create sandboxes exclude SQL snippets.	.com/metabase/metabase/pull/30854	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32680		
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.44.7					
Missing Authentication for Critical Function	18-May-2023	9.6	Metabase is an open source business analytics engine. To edit SQL Snippets, Metabase should have required people to be in at least one group with native query editing permissions to a database–but affected versions of Metabase didn't enforce that requirement. This lack of enforcement meant that: Anyone–including people in sandboxed groups–could edit SQL snippets. They could edit snippets via the API or, in the application UI, when editing the metadata for a model based on a SQL question, and people in sandboxed groups could edit a SQL snippet used in a query that creates their sandbox. If the snippet contained logic that restricted which data that person could see,	https://github.com/metabase/metabase/pull/30852, https://github.com/metabase/metabase/security/advisories/GHSA-mw6j-f894-4qxv, https://github.com/metabase/metabase/pull/30853, https://github.com/metabase/metabase/pull/30854	A-MET-META-020623/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			they could potentially edit that snippet and change their level of data access. The permissions model for SQL snippets has been fixed in Metabase versions 0.46.3, 0.45.4, 0.44.7, 1.46.3, 1.45.4, and 1.44.7. Users are advised to upgrade. Users unable to upgrade should ensure that SQL queries used to create sandboxes exclude SQL snippets. **CVE ID : CVE-2023-32680**		
Affected Version(s): From (including) 1.45.0 Up to (excluding) 1.45.4					
Missing Authentication for Critical Function	18-May-2023	9.6	Metabase is an open source business analytics engine. To edit SQL Snippets, Metabase should have required people to be in at least one group with native query editing permissions to a database–but affected versions of Metabase didn't enforce that requirement. This lack of enforcement meant that: Anyone–including people in	https://github.com/metabase/metabase/pull/30852, https://github.com/metabase/metabase/security/advisories/GHSA-mw6j-f894-4qxv, https://github.com/metabase/metabase/pull/30853, https://github.com/metabase/metabase/pull/30854	A-MET-META-020623/349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sandboxed groups– could edit SQL snippets. They could edit snippets via the API or, in the application UI, when editing the metadata for a model based on a SQL question, and people in sandboxed groups could edit a SQL snippet used in a query that creates their sandbox. If the snippet contained logic that restricted which data that person could see, they could potentially edit that snippet and change their level of data access. The permissions model for SQL snippets has been fixed in Metabase versions 0.46.3, 0.45.4, 0.44.7, 1.46.3, 1.45.4, and 1.44.7. Users are advised to upgrade. Users unable to upgrade should ensure that SQL queries used to create sandboxes exclude SQL snippets. **CVE ID : CVE-2023-32680**		
Affected Version(s): From (including) 1.46.0 Up to (excluding) 1.46.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	18-May-2023	9.6	Metabase is an open source business analytics engine. To edit SQL Snippets, Metabase should have required people to be in at least one group with native query editing permissions to a database–but affected versions of Metabase didn't enforce that requirement. This lack of enforcement meant that: Anyone–including people in sandboxed groups–could edit SQL snippets. They could edit snippets via the API or, in the application UI, when editing the metadata for a model based on a SQL question, and people in sandboxed groups could edit a SQL snippet used in a query that creates their sandbox. If the snippet contained logic that restricted which data that person could see, they could potentially edit that snippet and change their level of data	https://github.com/metabase/metabase/pull/30852, https://github.com/metabase/metabase/security/advisories/GHSA-mw6j-f894-4qxv, https://github.com/metabase/metabase/pull/30853, https://github.com/metabase/metabase/pull/30854	A-MET-META-020623/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access. The permissions model for SQL snippets has been fixed in Metabase versions 0.46.3, 0.45.4, 0.44.7, 1.46.3, 1.45.4, and 1.44.7. Users are advised to upgrade. Users unable to upgrade should ensure that SQL queries used to create sandboxes exclude SQL snippets. **CVE ID : CVE-2023-32680**		
Vendor: metagauss					
Product: registrationmagic					
Affected Version(s): * Up to (including) 5.2.0.5					
Authorization Bypass Through User-Controlled Key	16-May-2023	7.2	The RegistrationMagic plugin for WordPress is vulnerable to Insecure Direct Object References in versions up to, and including, 5.2.0.5. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for authenticated attackers, with	https://plugins.trac.wordpress.org/browser/custom-registration-form-builder-with-submission-manager/tags/5.2.0.5/includes/class_rm_utilities.php#L3044	A-MET-REGI-020623/351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			administrator-level permissions and above, to change user passwords and potentially take over super-administrator accounts in multisite setup. **CVE ID : CVE-2023-2548**		
Affected Version(s): * Up to (including) 5.2.1.0					
Improper Authentication	16-May-2023	9.8	The RegistrationMagic plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 5.2.1.0. This is due to insufficient verification on the user being supplied during a Google social login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email. **CVE ID : CVE-2023-2499**	https://plugins.trac.wordpress.org/browser/custom-registration-form-builder-with-submission-manager/tags/5.2.0.4/services/class_rm_user_services.php#L791	A-MET-REGI-020623/352
Vendor: microengine					
Product: mailform					
Affected Version(s): From (including) 1.1.0 Up to (excluding) 1.1.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	23-May-2023	9.8	Unrestricted upload of file with dangerous type exists in MicroEngine Mailform version 1.1.0 to 1.1.8. If the product's file upload function and server save option are enabled, a remote attacker may save an arbitrary file on the server and execute it. **CVE ID : CVE-2023-27397**	https://microengine.jp/information/security_2023_05.html	A-MIC-MAIL-020623/353
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-May-2023	9.8	MicroEngine Mailform version 1.1.0 to 1.1.8 contains a path traversal vulnerability. If the product's file upload function and server save option are enabled, a remote attacker may save an arbitrary file on the server and execute it. **CVE ID : CVE-2023-27507**	https://microengine.jp/information/security_2023_05.html	A-MIC-MAIL-020623/354
Vendor: mijnpress					
Product: auto_prune_posts					
Affected Version(s): * Up to (excluding) 2.0.0					
Cross-Site Request	18-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Ramon Fincken	N/A	A-MIJ-AUTO-020623/355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			Auto Prune Posts plugin <= 1.8.0 versions. **CVE ID : CVE-2023-27423**		
Product: mass_delete_unused_tags					
Affected Version(s): * Up to (excluding) 3.0.0					
Cross-Site Request Forgery (CSRF)	18-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Ramon Fincken Mass Delete Unused Tags plugin <= 2.0.0 versions. **CVE ID : CVE-2023-27430**	N/A	A-MIJ-MASS-020623/356
Vendor: miktex					
Product: miktex					
Affected Version(s): From (including) 2.9.6300 Up to (excluding) 23.5					
N/A	20-May-2023	7.8	LuaTeX before 1.17.0 allows execution of arbitrary shell commands when compiling a TeX file obtained from an untrusted source. This occurs because luatex-core.lua lets the original io.popen be accessed. This also affects TeX Live before 2023 r66984 and MiKTeX before 23.5. **CVE ID : CVE-2023-32700**	https://tug.org/~mseven/luatex.html	A-MIK-MIKT-020623/357
Vendor: miniorange					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wordpress_social_login_and_register_\(discord\,_google\,_twitter\,_linkedin\)					
Affected Version(s): * Up to (excluding) 7.6.0					
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in miniOrange WordPress Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin <= 7.5.14 versions. **CVE ID : CVE-2023-23706**	N/A	A-MIN-WORD-020623/358
Vendor: minovateknoloji					
Product: etrace					
Affected Version(s): * Up to (excluding) 23.05.20					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-May-2023	9.8	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Minova Technology eTrace allows SQL Injection.This issue affects eTrace: before 23.05.20. **CVE ID : CVE-2023-2064**	N/A	A-MIN-ETRA-020623/359
Vendor: mipjz_project					
Product: mipjz					
Affected Version(s): 5.0.5					
Improper Neutralization of	25-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in	N/A	A-MIP-MIPJ-020623/360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			mipjz v5.0.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Description parameter at /index.php?s=/article/ApiAdminArticle/itemAdd. **CVE ID : CVE-2023-33750**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in mipjz v5.0.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the name parameter at /app/tag/controller/ApiAdminTagCategory.php. **CVE ID : CVE-2023-33751**	N/A	A-MIP-MIPJ-020623/361
Vendor: Mitel					
Product: mivoice_connect					
Affected Version(s): * Up to (including) 22.24.1500.0					
N/A	24-May-2023	9.8	A vulnerability in the Headquarters server component of Mitel MiVoice Connect versions 19.3 SP2 (22.24.1500.0) and earlier could allow an unauthenticated attacker with internal network	https://www.mitel.com/support/security-advisories, https://www.mitel.com/support/security-advisories/mitel-product-security-	A-MIT-MIVO-020623/362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to execute arbitrary scripts due to improper access control. **CVE ID : CVE-2023-31457**	advisory-23-0004	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	6.1	A vulnerability in the conferencing component of Mitel MiVoice Connect through 19.3 SP2 and 20.x, 21.x, and 22.x through 22.24.1500.0 could allow an unauthenticated attacker to conduct a reflected cross-site scripting (XSS) attack due to insufficient validation for the home.php page. A successful exploit could allow an attacker to execute arbitrary scripts. **CVE ID : CVE-2023-25598**	https://www.mitel.com/support/security-advisories, https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-23-0003	A-MIT-MIVO-020623/363
Affected Version(s): * Up to (including) 9.6.2208.101					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-May-2023	7.2	A vulnerability in the Connect Mobility Router component of MiVoice Connect versions 9.6.2208.101 and earlier could allow an authenticated attacker with internal network access to conduct a	https://www.mitel.com/support/security-advisories, https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-23-0007	A-MIT-MIVO-020623/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			command injection attack due to insufficient restriction on URL parameters. **CVE ID : CVE-2023-31460**		
Vendor: mobilemouse					
Product: mobile_mouse					
Affected Version(s): 3.6.0.4					
N/A	17-May-2023	9.8	RPA Technology Mobile Mouse 3.6.0.4 is vulnerable to Remote Code Execution (RCE). **CVE ID : CVE-2023-31902**	N/A	A-MOB-MOBI-020623/365
Vendor: monsterinsights					
Product: google_analytics_dashboard					
Affected Version(s): * Up to (excluding) 8.14.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in MonsterInsights plugin <= 8.14.0 versions. **CVE ID : CVE-2023-23999**	N/A	A-MON-GOOG-020623/366
Vendor: morosystems					
Product: easymind					
Affected Version(s): * Up to (excluding) 2.15.0					
Improper Neutralization of Input During	17-May-2023	5.4	The MoroSystems EasyMind - Mind Maps plugin before 2.15.0 for Confluence allows	N/A	A-MOR-EASY-020623/367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			persistent XSS when saving a Mind Map with the hyperlink parameter. **CVE ID : CVE-2023-30452**		
Vendor: Moxa					
Product: mxsecurity					
Affected Version(s): 1.0					
Use of Hard-coded Credentials	22-May-2023	9.8	MXsecurity version 1.0 is vulnearble to hardcoded credential vulnerability. This vulnerability has been reported that can be exploited to craft arbitrary JWT tokens and subsequently bypass authentication for web-based APIs. **CVE ID : CVE-2023-33236**	https://www.moxa.com/en/support/product-support/security-advisory/mxsecurity-command-injection-and-hardcoded-credential-vulnerabilities	A-MOX-MXSE-020623/368
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-2023	8.8	MXsecurity version 1.0 is vulnearble to command injection vulnerability. This vulnerability has been reported in the SSH CLI program, which can be exploited by attackers who have gained authorization privileges. The attackers can break	https://www.moxa.com/en/support/product-support/security-advisory/mxsecurity-command-injection-and-hardcoded-credential-vulnerabilities	A-MOX-MXSE-020623/369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			out of the restricted shell and subsequently execute arbitrary code. **CVE ID : CVE-2023-33235**		
Vendor: mw_wp_form_project					
Product: mw_wp_form					
Affected Version(s): * Up to (including) 4.4.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-May-2023	9.8	Directory traversal vulnerability in MW WP Form versions v4.4.2 and earlier allows a remote unauthenticated attacker to alter the website or cause a denial-of-service (DoS) condition, and obtain sensitive information depending on settings. **CVE ID : CVE-2023-28408**	https://plugins.2inc.org/mw-wp-form/blog/2023/05/08/752/	A-MW_-MW_W-020623/370
Unrestricted Upload of File with Dangerous Type	23-May-2023	9.8	Unrestricted upload of file with dangerous type exists in MW WP Form versions v4.4.2 and earlier, which may allow a remote unauthenticated attacker to upload an arbitrary file.	https://plugins.2inc.org/mw-wp-form/blog/2023/05/08/752/	A-MW_-MW_W-020623/371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28409		
Vendor: Mybb					
Product: mybb					
Affected Version(s): * Up to (excluding) 1.8.34					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-May-2023	6.1	In MyBB before 1.8.34, there is XSS in the User CP module via the user email field. **CVE ID : CVE-2023-28467**	https://github.com/mybb/mybb/security/advisories/GHSA-3q8x-9fh2-v646	A-MYB-MYBB-020623/372
Vendor: my_calendar_project					
Product: my_calendar					
Affected Version(s): * Up to (including) 3.4.3					
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Joseph C Dolson My Calendar plugin <= 3.4.3 versions. **CVE ID : CVE-2023-23813**	N/A	A-MY_-MY_C-020623/373
Vendor: name_directory_project					
Product: name_directory					
Affected Version(s): * Up to (including) 1.27.1					
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Jeroen Peters Name Directory plugin <= 1.27.1 versions. **CVE ID : CVE-2023-22692**	N/A	A-NAM-NAME-020623/374
Vendor: Nasm					
Product: netwide_assembler					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 2.16.02					
Out-of-bounds Write	17-May-2023	7.8	There exists a heap buffer overflow in nasm 2.16.02rc1 (GitHub commit: b952891). **CVE ID : CVE-2023-31722**	https://bugzilla.nasm.us/show_bug.cgi?id=3392857#c1	A-NAS-NETW-020623/375
Vendor: netbox_project					
Product: netbox					
Affected Version(s): 3.5.1					
N/A	24-May-2023	9.1	** DISPUTED ** A vulnerability in Netbox v3.5.1 allows unauthenticated attackers to execute queries against the GraphQL database, granting them access to sensitive data stored in the database. NOTE: the vendor disputes this because the reporter's only query was for the schema of the API, which is public; queries for database objects would have been denied. **CVE ID : CVE-2023-33796**	N/A	A-NET-NETB-020623/376
Improper Neutralization of Input During Web Page	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Rack Roles (/dcim/rack-roles/) function of	N/A	A-NET-NETB-020623/377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33785**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Circuit Types (/circuits/circuit-types/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33786**	N/A	A-NET-NETB-020623/378
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Tenant Groups (/tenancy/tenant-groups/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33787**	N/A	A-NET-NETB-020623/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Providers (/circuits/providers/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33788**	N/A	A-NET-NETB-020623/380
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Contact Groups (/tenancy/contact-groups/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33789**	N/A	A-NET-NETB-020623/381
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Locations (/dcim/locations/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload	N/A	A-NET-NETB-020623/382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			injected into the Name field. **CVE ID : CVE-2023-33790**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Provider Accounts (/circuits/provider-accounts/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33791**	N/A	A-NET-NETB-020623/383
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Site Groups (/dcim/site-groups/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33792**	N/A	A-NET-NETB-020623/384
Improper Neutralization of Input During Web Page	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Power Panels (/dcim/power-	N/A	A-NET-NETB-020623/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			panels/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33793**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Tenants (/tenancy/tenants/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33794**	N/A	A-NET-NETB-020623/386
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Contact Roles (/tenancy/contact-roles/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33795**	N/A	A-NET-NETB-020623/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Sites (/dcim/sites/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33797**	N/A	A-NET-NETB-020623/388
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Rack (/dcim/rack/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33798**	N/A	A-NET-NETB-020623/389
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Contacts (/tenancy/contacts/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted	N/A	A-NET-NETB-020623/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			payload injected into the Name field. **CVE ID : CVE-2023-33799**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	5.4	A stored cross-site scripting (XSS) vulnerability in the Create Regions (/dcim/regions/) function of Netbox v3.5.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field. **CVE ID : CVE-2023-33800**	N/A	A-NET-NETB-020623/391
Vendor: obsidian					
Product: obsidian					
Affected Version(s): * Up to (excluding) 1.2.2					
N/A	20-May-2023	8.2	Obsidian before 1.2.2 allows calls to unintended APIs (for microphone access, camera access, and desktop notification) via an embedded web page. **CVE ID : CVE-2023-33244**	N/A	A-OBS-OBSI-020623/392
Vendor: old_age_home_management_system_project					
Product: old_age_home_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special	23-May-2023	9.8	Old Age Home Management 1.0 is vulnerable to SQL Injection via the	N/A	A-OLD-OLD_-020623/393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			username parameter. **CVE ID : CVE-2023-33338**		
Vendor: ombi					
Product: ombi					
Affected Version(s): * Up to (excluding) 4.38.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-May-2023	4.9	Ombi is an open source application which allows users to request specific media from popular self-hosted streaming servers. Versions prior to 4.38.2 contain an arbitrary file read vulnerability where an Ombi administrative user may access files available to the Ombi server process on the host operating system. Ombi administrators may not always be local system administrators and so this may violate the security expectations of the system. The arbitrary file read vulnerability was present in `ReadLogFile` and `Download` endpoints in `SystemControllers.	https://github.com/Ombi-app/Ombi/commit/b8a8f029d80454d582bc4a2a05175106809335d0	A-OMB-OMBI-020623/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cs` as the parameter `logFileName` is not sanitized before being combined with the `Logs` directory. When using `Path.Combine(arg 1, arg2, arg3)`, an attacker may be able to escape to folders/files outside of `Path.Combine(arg 1, arg2)` by using ".." in `arg3`. In addition, by specifying an absolute path for `arg3`, `Path.Combine` will completely ignore the first two arguments and just return just `arg3`. This vulnerability can lead to information disclosure. The Ombi `documentation` suggests running Ombi as a Service with Administrator privileges. An attacker targeting such an application may be able to read the files of any Windows user on the host machine and certain system files. This issue has		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been addressed in commit `b8a8f029` and in release version 4.38.2. Users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as GHSL-2023-088. **CVE ID : CVE-2023-32322**		
Vendor: online_computer_and_laptop_store_project					
Product: online_computer_and_laptop_store					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	16-May-2023	9.8	Sourcecodester Online Computer and Laptop Store 1.0 allows unrestricted file upload and can lead to remote code execution. The vulnerability path is /classes/Users.php?f=save. **CVE ID : CVE-2023-31857**	N/A	A-ONL-ONLI-020623/395
Vendor: online_exam_system_project					
Product: online_exam_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements	17-May-2023	8.8	A vulnerability classified as critical was found in SourceCodester Online Exam	N/A	A-ONL-ONLI-020623/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			System 1.0. This vulnerability affects unknown code of the file /kelasdosen/data. The manipulation of the argument columns[1][data] leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229276. **CVE ID : CVE-2023-2770**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-2023	8.8	A vulnerability, which was classified as critical, has been found in SourceCodester Online Exam System 1.0. This issue affects some unknown processing of the file /jurusanmatkul/data. The manipulation of the argument columns[1][data] leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to	N/A	A-ONL-ONLI-020623/397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the public and may be used. The identifier VDB-229277 was assigned to this vulnerability. **CVE ID : CVE-2023-2771**		
Vendor: online_jewelry_store_project					
Product: online_jewelry_store					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-May-2023	9.8	A vulnerability classified as critical was found in SourceCodester Online Jewelry Store 1.0. Affected by this vulnerability is an unknown functionality of the file supplier.php of the component POST Parameter Handler. The manipulation of the argument suppid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-229429 was assigned to this vulnerability. **CVE ID : CVE-2023-2815**	N/A	A-ONL-ONLI-020623/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	6.1	A vulnerability was found in SourceCodester Online Jewelry Store 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file customer.php of the component POST Parameter Handler. The manipulation of the argument Custid leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229820. **CVE ID : CVE-2023-2864**	N/A	A-ONL-ONLI-020623/399
Vendor: Open-emr					
Product: openemr					
Affected Version(s): * Up to (excluding) 7.0.1					
Improper Control of Generation of Code ('Code Injection')	27-May-2023	8.8	Code Injection in GitHub repository openemr/openemr prior to 7.0.1. **CVE ID : CVE-2023-2943**	https://github.com/openemr/openemr/commit/c1c0805696ca68577c37bf30e29f90e5f3e0f1a9, https://huntr.dev/bounties/	A-OPE-OPEN-020623/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				4190f944-dc2c-4624-9abf-31479456faa9	
Improper Input Validation	27-May-2023	8.1	Improper Input Validation in GitHub repository openemr/openemr prior to 7.0.1. **CVE ID : CVE-2023-2942**	https://github.com/openemr/openemr/commit/c1c0805696ca68577c37bf30e29f90e5f3e0f1a9, https://huntr.dev/bounties/dd56e7a0-9dff-48fc-bc59-9a22d91869eb	A-OPE-OPEN-020623/401
Improper Access Control	27-May-2023	8.1	Improper Access Control in GitHub repository openemr/openemr prior to 7.0.1. **CVE ID : CVE-2023-2946**	https://huntr.dev/bounties/e550f4b0-945c-4886-af7f-ee0dc30b2a08, https://github.com/openemr/openemr/commit/81832acc14207e577e76c4175967c99ae7e3d3f4	A-OPE-OPEN-020623/402
Improper Authorization	28-May-2023	8.1	Improper Authorization in GitHub repository openemr/openemr prior to 7.0.1. **CVE ID : CVE-2023-2950**	https://github.com/openemr/openemr/commit/abee8d2606c706176818de25eb88a2d08b8f7fa4, https://huntr.dev/bounties/612d13cf-2ef9-44ea-	A-OPE-OPEN-020623/403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				b8fb-e797948a9a86	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-May-2023	6.1	Cross-site Scripting (XSS) - Generic in GitHub repository openemr/openemr prior to 7.0.1. **CVE ID : CVE-2023-2948**	https://github.com/openemr/openemr/commit/af1ecf78d1342519791bda9d3079e88f7d859015, https://huntr.dev/bounties/2393e4d9-9e9f-455f-bf50-f20f77b0a64d	A-OPE-OPEN-020623/404
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-May-2023	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.1. **CVE ID : CVE-2023-2949**	https://huntr.dev/bounties/3842486f-38b1-4150-9f78-b81d0ae580c4, https://github.com/openemr/openemr/commit/af1ecf78d1342519791bda9d3079e88f7d859015	A-OPE-OPEN-020623/405
Improper Access Control	27-May-2023	5.4	Improper Access Control in GitHub repository openemr/openemr prior to 7.0.1. **CVE ID : CVE-2023-2944**	https://github.com/openemr/openemr/commit/723ac5d78080d1b8542f47673988cd63e0389d25, https://huntr.dev/bounties/0d67dcb1-acc0-4d5d-	A-OPE-OPEN-020623/406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				bb69-a09d1bc9fa1d	
Missing Authorization	27-May-2023	5.4	Missing Authorization in GitHub repository openemr/openemr prior to 7.0.1. **CVE ID : CVE-2023-2945**	https://huntr.dev/bounties/62de71bd-333d-4593-91a5-534ef7f0c435, https://github.com/openemr/openemr/commit/3656bc88288957d68ba040cad2e5f9dbd1b607b1	A-OPE-OPEN-020623/407
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-May-2023	4.8	Cross-site Scripting (XSS) - Stored in GitHub repository openemr/openemr prior to 7.0.1. **CVE ID : CVE-2023-2947**	https://github.com/openemr/openemr/commit/8d2d601ac40aca75bcd2c3cf193f59c8e56d8425, https://huntr.dev/bounties/52534def-acab-4200-a79a-89ef4ce6a0b0	A-OPE-OPEN-020623/408
Vendor: Opentext					
Product: documentum_content_server					
Affected Version(s): * Up to (excluding) 23.2					
N/A	18-May-2023	7.8	OpenText Documentum Content Server before 23.2 has a flaw that allows for privilege escalation from a non-privileged Documentum user to root. The software comes	N/A	A-OPE-DOCU-020623/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prepackaged with a root owned SUID binary dm_secure_writer. The binary has security controls in place preventing creation of a file in a non-owned directory, or as the root user. However, these controls can be carefully bypassed to allow for an arbitrary file write as root. **CVE ID : CVE-2023-31871**		
Vendor: perfree					
Product: perfreeblog					
Affected Version(s): 3.1.2					
Unrestricted Upload of File with Dangerous Type	18-May-2023	9.8	An arbitrary file upload vulnerability in the component /admin/ThemeController.java of PerfreeBlog v3.1.2 allows attackers to execute arbitrary code via a crafted file. **CVE ID : CVE-2023-30333**	N/A	A-PER-PERF-020623/410
Vendor: pharmacy_management_system_project					
Product: pharmacy_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special	16-May-2023	9.8	Pharmacy Management System v1.0 was discovered to	N/A	A-PHA-PHAR-020623/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			contain a SQL injection vulnerability via the email parameter at login_core.php. **CVE ID : CVE-2023-31519**		
Vendor: Phpmyfaq					
Product: phpmyfaq					
Affected Version(s): * Up to (excluding) 3.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.0-beta. **CVE ID : CVE-2023-2752**	https://huntr.dev/bounties/efdf5b24-6d30-4d57-a5b0-13b253ba3ea4, https://github.com/thorsten/phpmyfaq/commit/e7599d49b0ece7ceef3a4e8d334782cc3df98be8	A-PHP-PHPM-020623/412
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.0-beta. **CVE ID : CVE-2023-2753**	https://github.com/thorsten/phpmyfaq/commit/5401ab75d022932b8d5d7adaa771acf44fed18ba, https://huntr.dev/bounties/eca2284d-e81a-4ab8-91bb-7afeca557628	A-PHP-PHPM-020623/413
Affected Version(s): 3.2.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.0-beta. **CVE ID : CVE-2023-2752**	https://huntr.dev/bounties/efdf5b24-6d30-4d57-a5b0-13b253ba3ea4, https://github.com/thorsten/phpmyfaq/commit/e7599d49b0ece7ceef3a4e8d334782cc3df98be8	A-PHP-PHPM-020623/414
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.0-beta. **CVE ID : CVE-2023-2753**	https://github.com/thorsten/phpmyfaq/commit/5401ab75d022932b8d5d7adaa771acf44fed18ba, https://huntr.dev/bounties/eca2284d-e81a-4ab8-91bb-7afeca557628	A-PHP-PHPM-020623/415
Vendor: Pimcore					
Product: customer-data-framework					
Affected Version(s): * Up to (excluding) 3.3.10					
Insufficiently Protected Credentials	25-May-2023	4.9	Storing Passwords in a Recoverable Format in GitHub repository pimcore/customer-data-framework prior to 3.3.10. **CVE ID : CVE-2023-2881**	https://huntr.dev/bounties/db6c32f4-742e-4262-8fd5-cefd0f133416, https://github.com/pimcore/customer-data-framework/co	A-PIM-CUST-020623/416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				mmit/d1d58c10313f080737dc1e71fab3beb12488a1e6	
Product: customer_management_framework					
Affected Version(s): * Up to (excluding) 3.3.10					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-2023	7.2	SQL Injection in GitHub repository pimcore/customer-data-framework prior to 3.3.10. **CVE ID : CVE-2023-2756**	https://github.com/pimcore/customer-data-framework/commit/76df151737b7964ce5169fdf9e27a0ad801757fe, https://huntr.dev/bounties/cf398528-819f-456e-88e7-c06d268d3f44	A-PIM-CUST-020623/417
Product: pimcore					
Affected Version(s): * Up to (excluding) 10.3.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.3.3. **CVE ID : CVE-2023-2730**	https://huntr.dev/bounties/6c6f5c26-d545-4e7b-82bb-1fe28006c885, https://github.com/pimcore/pimcore/commit/8ab06bfbb5a05a1b190731d9c7476ec45f5ee878	A-PIM-PIMC-020623/418
Vendor: pingonline					
Product: dyslexiefont_free					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.0.0					
Cross-Site Request Forgery (CSRF)	20-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in PingOnline Dyslexiefont Free plugin <= 1.0.0 versions. **CVE ID : CVE-2023-32589**	N/A	A-PIN-DYSL-020623/419
Vendor: Piwigo					
Product: piwigo					
Affected Version(s): * Up to (excluding) 13.6.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-2023	8.8	Piwigo before 13.6.0 was discovered to contain a SQL injection vulnerability via the order[0][dir] parameter at user_list_backend.php. **CVE ID : CVE-2023-27233**	https://github.com/Piwigo/Piwigo/issues/1872	A-PIW-PIWI-020623/420
Affected Version(s): 13.6.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-May-2023	9.8	Piwigo 13.6.0 is vulnerable to SQL Injection via /admin/permalinks.php. **CVE ID : CVE-2023-33361**	https://github.com/Piwigo/Piwigo/issues/1910	A-PIW-PIWI-020623/421
Improper Neutralization of Special Elements	23-May-2023	9.8	Piwigo 13.6.0 is vulnerable to SQL Injection via in the "profile" function.	https://github.com/Piwigo/Piwigo/issues/1911	A-PIW-PIWI-020623/422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			**CVE ID : CVE-2023-33362**		
Cross-Site Request Forgery (CSRF)	23-May-2023	4.3	Piwigo 13.6.0 is vulnerable to Cross Site Request Forgery (CSRF) in the "add tags" function. **CVE ID : CVE-2023-33359**	N/A	A-PIW-PIWI-020623/423
Vendor: plugin					
Product: waiting					
Affected Version(s): * Up to (including) 0.6.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-May-2023	5.4	The Waiting: One-click countdowns plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on 'saveLang' functions in versions up to, and including, 0.6.2. This could lead to Cross-Site Scripting due to insufficient input sanitization and output escaping. This makes it possible for subscriber-level attackers to access functions to save plugin data that can potentially lead to inject arbitrary web scripts in pages	N/A	A-PLU-WAIT-020623/424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that will execute whenever a user accesses an injected page. **CVE ID : CVE-2023-2757**		
Vendor: podlove					
Product: podlove_podcast_publisher					
Affected Version(s): * Up to (excluding) 3.8.4					
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Podlove Podlove Podcast Publisher plugin <= 3.8.3 versions. **CVE ID : CVE-2023-25472**	N/A	A-POD-PODL-020623/425
Product: podlove_subscribe_button					
Affected Version(s): * Up to (excluding) 1.3.9					
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Podlove Podlove Subscribe button plugin <= 1.3.7 versions. **CVE ID : CVE-2023-25481**	N/A	A-POD-PODL-020623/426
Vendor: posthemes					
Product: posstaticblocks					
Affected Version(s): * Up to (including) 1.0.0					
Improper Neutralization of Special Elements used in an SQL	16-May-2023	9.8	Prestashop posstaticblocks <= 1.0.0 is vulnerable to SQL Injection via posstaticblocks::getPosCurrentHook().	https://friends-of-presta.github.io/security-advisories/modules/2023/0	A-POS-POSS-020623/427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			**CVE ID : CVE-2023-30189**	4/27/posstaticblocks.html	
Vendor: QT					
Product: qt					
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.15.4					
Out-of-bounds Read	22-May-2023	7.5	An issue was discovered in Qt 5.x before 5.15.14, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.1. QDnsLookup has a buffer over-read via a crafted reply from a DNS server. **CVE ID : CVE-2023-33285**	https://codereview.qt-project.org/c/qt/qtbase/+/477644	A-QT-QT-020623/428
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.2.9					
Out-of-bounds Read	22-May-2023	7.5	An issue was discovered in Qt 5.x before 5.15.14, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.1. QDnsLookup has a buffer over-read via a crafted reply from a DNS server. **CVE ID : CVE-2023-33285**	https://codereview.qt-project.org/c/qt/qtbase/+/477644	A-QT-QT-020623/429
Affected Version(s): From (including) 6.3.0 Up to (excluding) 6.5.1					
Out-of-bounds Read	22-May-2023	7.5	An issue was discovered in Qt 5.x before 5.15.14, 6.x before 6.2.9, and 6.3.x through 6.5.x before 6.5.1. QDnsLookup has a buffer over-read via	https://codereview.qt-project.org/c/qt/qtbase/+/477644	A-QT-QT-020623/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a crafted reply from a DNS server. **CVE ID : CVE-2023-33285**		
Vendor: Quest					
Product: kace_systems_deployment_appliance					
Affected Version(s): 9.0.146					
Incorrect Authorization	21-May-2023	6.5	There is an LDAP bind credentials exposure on KACE Systems Deployment and Remote Site appliances 9.0.146. The captured credentials may provide a higher privilege level on the Active Directory domain. To exploit this, an authenticated attacker edits the user-authentication settings to specify an attacker-controlled LDAP server, clicks the Test Settings button, and captures the cleartext credentials. **CVE ID : CVE-2023-33254**	N/A	A-QUE-KACE-020623/431
Vendor: rankmath					
Product: seo_pro					
Affected Version(s): * Up to (including) 3.0.35					
Improper Neutralization of	28-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability	N/A	A-RAN-SEO_-020623/432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			in One Rank Math SEO PRO plugin <= 3.0.35 versions. **CVE ID : CVE-2023-32800**		
Vendor: reactphp					
Product: http					
Affected Version(s): From (including) 0.8.0 Up to (excluding) 1.9.0					
N/A	17-May-2023	5.3	react/http is an event-driven, streaming HTTP client and server implementation for ReactPHP. Previous versions of ReactPHP's HTTP server component contain a potential DoS vulnerability that can cause high CPU load when processing large HTTP request bodies. This vulnerability has little to no impact on the default configuration, but can be exploited when explicitly using the RequestBodyBuffer Middleware with very large settings. This might lead to consuming large amounts of CPU time for processing requests and significantly delay or slow down the	https://github.com/reactphp/http/commit/9681f764b80c45ebfb5fe2ea7da5bd3babfcdcfd, https://github.com/reactphp/http/security/advisories/GHSA-95x4-j7vc-h8mf	A-REA-HTTP-020623/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			processing of legitimate user requests. This issue has been addressed in release 1.9.0. Users are advised to upgrade. Users unable to upgrade may keep the request body limited using RequestBodyBuffer Middleware with a sensible value which should mitigate the issue. An infrastructure or DevOps workaround could be to place a reverse proxy in front of the ReactPHP HTTP server to filter out any excessive HTTP request bodies. **CVE ID : CVE-2023-26044**		
Vendor: redis					
Product: redis					
Affected Version(s): 7.0.10					
N/A	18-May-2023	7.5	redis-7.0.10 was discovered to contain a segmentation violation. **CVE ID : CVE-2023-31655**	https://github.com/RedisLabs/redisraft/issues/608	A-RED-REDI-020623/434
Vendor: rental_module_project					
Product: rental_module					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 23.05.15					
Unrestricted Upload of File with Dangerous Type	20-May-2023	9.8	Unrestricted Upload of File with Dangerous Type vulnerability in "Rental Module" developed by third-party for Ideasoft's E-commerce Platform allows Command Injection, Using Malicious Files, Upload a Web Shell to a Web Server.This issue affects Rental Module: before 23.05.15. **CVE ID : CVE-2023-2712**	N/A	A-REN-RENT-020623/435
Authorization Bypass Through User-Controlled Key	20-May-2023	9.8	Authorization Bypass Through User-Controlled Key vulnerability in "Rental Module" developed by third-party for Ideasoft's E-commerce Platform allows Authentication Abuse, Authentication Bypass.This issue affects Rental Module: before 23.05.15.	N/A	A-REN-RENT-020623/436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2713		
Vendor: robosoft					
Product: robogallery					
Affected Version(s): * Up to (including) 3.2.11					
Cross-Site Request Forgery (CSRF)	20-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in RoboSoft Photo Gallery, Images, Slider in Rbs Image Gallery plugin <= 3.2.11 versions. **CVE ID : CVE-2023-24414**	N/A	A-ROB-ROBO-020623/437
Vendor: S9Y					
Product: serendipity					
Affected Version(s): 2.4.0					
Unrestricted Upload of File with Dangerous Type	16-May-2023	8.8	An arbitrary file upload vulnerability in Serendipity 2.4-beta1 allows attackers to execute arbitrary code via a crafted HTML or Javascript file. **CVE ID : CVE-2023-31576**	N/A	A-S9Y-SERE-020623/438
Vendor: Sage					
Product: sage_300					
Affected Version(s): * Up to (including) 2022					
N/A	16-May-2023	4.3	Versions of Sage 300 through 2022 implement role-based access controls that are only enforced client-side. Low-	N/A	A-SAG-SAGE-020623/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileged Sage users, particularly those on a workstation setup in the "Windows Peer-to-Peer Network" or "Client Server Network" Sage 300 configurations, could recover the SQL connection strings being used by Sage 300 and interact directly with the underlying database(s) to create, update, and delete all company records, bypassing the program's role-based access controls. **CVE ID : CVE-2023-29927**		
Vendor: Savysoda					
Product: wifi_hd_wireless_disk_drive					
Affected Version(s): 11					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	7.5	savysoda Wifi HD Wireless Disk Drive 11 is vulnerable to Local File Inclusion. **CVE ID : CVE-2023-31904**	N/A	A-SAV-WIFI-020623/440
Vendor: Schneider-electric					
Product: opc_factory_server					
Affected Version(s): * Up to (excluding) 3.63					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference	16-May-2023	5.5	A CWE-611: Improper Restriction of XML External Entity Reference vulnerability exists that could cause unauthorized read access to the file system when a malicious configuration file is loaded on to the software by a local user. **CVE ID : CVE-2023-2161**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-129-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-129-01.pdf	A-SCH-OPC_-020623/441
Affected Version(s): 3.63					
Improper Restriction of XML External Entity Reference	16-May-2023	5.5	A CWE-611: Improper Restriction of XML External Entity Reference vulnerability exists that could cause unauthorized read access to the file system when a malicious configuration file is loaded on to the software by a local user. **CVE ID : CVE-2023-2161**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-129-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-129-01.pdf	A-SCH-OPC_-020623/442
Vendor: secondlinethemes					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: auto_youtube_importer					
Affected Version(s): * Up to (excluding) 1.0.4					
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in SecondLineThemes Auto YouTube Importer plugin <= 1.0.3 versions. **CVE ID : CVE-2023-23797**	N/A	A-SEC-AUTO-020623/443
Vendor: Sem-cms					
Product: Semcms					
Affected Version(s): 1.5					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-May-2023	9.8	SEMCMS 1.5 is vulnerable to SQL Injection via Ant_Rponse.php. **CVE ID : CVE-2023-31707**	N/A	A-SEM-SEMC-020623/444
Vendor: service_provider_management_system_project					
Product: service_provider_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-May-2023	8.8	A vulnerability classified as critical has been found in SourceCodester Service Provider Management System 1.0. This affects an unknown part of the file /classes/Master.php?f=delete_service. The manipulation of the argument id	N/A	A-SER-SERV-020623/445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-229275. **CVE ID : CVE-2023-2769**		
Vendor: silabs					
Product: gecko_software_development_kit					
Affected Version(s): * Up to (including) 4.2.1					
N/A	18-May-2023	7.5	Compiler removal of buffer clearing in sli_cryptoacc_transparent_key_agreement in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM. **CVE ID : CVE-2023-0965**	N/A	A-SIL-GECK-020623/446
N/A	18-May-2023	7.5	Compiler removal of buffer clearing in sli_se_driver_key_agreement	N/A	A-SIL-GECK-020623/447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM. **CVE ID : CVE-2023-1132**		
N/A	18-May-2023	7.5	Compiler removal of buffer clearing in sli_se_opaque_import_key in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM. **CVE ID : CVE-2023-2481**	N/A	A-SIL-GECK-020623/448
N/A	18-May-2023	7.5	Compiler removal of buffer clearing in	N/A	A-SIL-GECK-020623/449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sli_crypto_transparent_aead_encrypt_tag in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM. **CVE ID : CVE-2023-32096**		
N/A	18-May-2023	7.5	Compiler removal of buffer clearing in sli_crypto_transparent_aead_decrypt_tag in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM.	N/A	A-SIL-GECK-020623/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-32097		
N/A	18-May-2023	7.5	Compiler removal of buffer clearing in sli_se_sign_message in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM. **CVE ID : CVE-2023-32098**	N/A	A-SIL-GECK-020623/451
N/A	18-May-2023	7.5	Compiler removal of buffer clearing in	N/A	A-SIL-GECK-020623/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sli_se_sign_hash in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM. **CVE ID : CVE-2023-32099**		
N/A	18-May-2023	7.5	Compiler removal of buffer clearing in sli_se_driver_mac_compute in Silicon Labs Gecko Platform SDK v4.2.1 and earlier results in key material duplication to RAM. **CVE ID : CVE-2023-32100**	N/A	A-SIL-GECK-020623/453
Vendor: silicon_project					
Product: silicon					
Affected Version(s): -					
Improper Neutralization of	22-May-2023	6.1	GitHub repository cu/silicon commit a9ef36 was	N/A	A-SIL-SILI-020623/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			discovered to contain a reflected cross-site scripting (XSS) vulnerability via the User Input field. **CVE ID : CVE-2023-31584**		
Vendor: simpledesign					
Product: diary_with_lock					
Affected Version(s): _daily_journal					
Cleartext Storage of Sensitive Information	24-May-2023	5.5	A vulnerability has been found in Simple Design Daily Journal 1.012.GP.B on Android and classified as problematic. Affected by this vulnerability is an unknown functionality of the component SQLite Database. The manipulation leads to cleartext storage in a file or on disk. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-229819. **CVE ID : CVE-2023-2863**	N/A	A-SIM-DIAR-020623/455
Vendor: simple_photo_gallery_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: simple_photo_gallery					
Affected Version(s): 1.0					
Unrestricted Upload of File with Dangerous Type	17-May-2023	9.8	A vulnerability was found in code-projects Simple Photo Gallery 1.0. It has been declared as critical. This vulnerability affects unknown code. The manipulation leads to unrestricted upload. The attack can be initiated remotely. VDB-229282 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-2776**	N/A	A-SIM-SIMP-020623/456
Vendor: Sitecore					
Product: experience_platform					
Affected Version(s): * Up to (excluding) 10.2					
Deserialization of Untrusted Data	23-May-2023	9.8	Deserialization of Untrusted Data in Sitecore Experience Platform through 10.2 allows remote attackers to run arbitrary code via ValidationResult.aspx. **CVE ID : CVE-2023-27068**	N/A	A-SIT-EXPE-020623/457
Affected Version(s): * Up to (including) 10.2					
Improper Limitation of a Pathname to a	22-May-2023	7.5	Directory Traversal vulnerability in Sitecore Experience Platform through 10.2 allows remote	https://blogs.night-wolf.io/0-day-vulnerabilities	A-SIT-EXPE-020623/458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			attackers to download arbitrary files via crafted command to download.aspx **CVE ID : CVE-2023-27067**	-at-sitecore-pagedesigner	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-May-2023	6.5	Directory Traversal vulnerability in Site Core Experience Platform 10.2 and earlier allows authenticated remote attackers to download arbitrary files via Urlhandle. **CVE ID : CVE-2023-27066**	https://blogs.night-wolf.io/0-day-vulnerabilities-at-sitecore-pagedesigner	A-SIT-EXPE-020623/459
Vendor: skeepers					
Product: verified_reviews_\(avis_verifies\)					
Affected Version(s): * Up to (including) 2.3.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in NetReviews SAS Verified Reviews (Avis Vérifiés) plugin <= 2.3.13 versions. **CVE ID : CVE-2023-23720**	N/A	A-SKE-VERI-020623/460
Vendor: skyscreamer					
Product: nevado_jms					
Affected Version(s): 1.3.2					
Missing Authorization	23-May-2023	7.8	Skyscreamer Open Source Nevado JMS v1.3.2 does not perform security checks when	N/A	A-SKY-NEVA-020623/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			receiving messages. This allows attackers to execute arbitrary commands via supplying crafted data. **CVE ID : CVE-2023-31826**		
Vendor: Slickremix					
Product: feed_them_social					
Affected Version(s): * Up to (excluding) 4.0.0					
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in SlickRemix Feed Them Social plugin <= 3.0.2 versions. **CVE ID : CVE-2023-25056**	N/A	A-SLI-FEED-020623/462
Vendor: Snapone					
Product: orvc					
Affected Version(s): * Up to (excluding) 7.2.0					
Use of Hard-coded Credentials	22-May-2023	9.8		N/A	A-SNA-ORVC-020623/463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snap One OvrC Pro versions prior to 7.2 have their own locally running web server accessible both from the local network and remotely. OvrC cloud contains a hidden superuser account accessible through hard-coded credentials.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31240		
Affected Version(s): * Up to (excluding) 7.3.0					
Insufficient Verification of Data Authenticity	22-May-2023	9.8	Snap One OvrC Pro devices versions 7.2 and prior do not	N/A	A-SNA-ORVC-020623/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware updates, resulting in code execution. **CVE ID : CVE-2023-28386**		
Improper Input Validation	22-May-2023	7.5	The Hub in the Snap One OvrC cloud platform is a device used to centralize and manage nested devices connected to it. A vulnerability exists in which an attacker could impersonate a hub and send device requests to claim already claimed devices. The OvrC	N/A	A-SNA-ORVC-020623/465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cloud platform receives the requests but does not validate if the found devices are already managed by another user. **CVE ID : CVE-2023-28649**		
Cleartext Transmission of Sensitive Information	22-May-2023	7.5	Snap One OvrC Pro versions prior to 7.3 use HTTP connections when downloading a program from their servers. Because they do not use	N/A	A-SNA-ORVC-020623/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			HTTPS, OvrC Pro devices are susceptible to exploitation. **CVE ID : CVE-2023-31193**		
N/A	22-May-2023	7.2		N/A	A-SNA-ORVC-020623/467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In Snap One OvrC Pro versions prior to 7.2, when logged into the superuser account, a new functionality appears that could allow users to execute arbitrary commands on the hub device.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25183		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1		N/A	A-SNA-ORVC-020623/468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31245		
Observable Discrepancy	22-May-2023	5.3	When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information.	N/A	A-SNA-ORVC-020623/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28412		
N/A	22-May-2023	10	Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright.	N/A	A-SNA-ORVC-020623/470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31241		
Vendor: snowsoftware					
Product: snow_license_manager					
Affected Version(s): From (including) 9.27 Up to (excluding) 9.30					
N/A	17-May-2023	4.3	Data leakage in Adobe connector in Snow Software SPE 9.27.0 on Windows allows privileged user to observe other users data. **CVE ID : CVE-2023-2679**	https://community.snowsoftware.com/s/feed/0D56M00009Ex9dySAB	A-SNO-SNOW-020623/471
Vendor: snow_monkey_forms_project					
Product: snow_monkey_forms					
Affected Version(s): * Up to (including) 5.0.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-May-2023	9.8	Directory traversal vulnerability in Snow Monkey Forms versions v5.0.6 and earlier allows a remote unauthenticated attacker to obtain sensitive information, alter the website, or cause a denial-of-service (DoS) condition. **CVE ID : CVE-2023-28413**	N/A	A-SNO-SNOW-020623/472
Vendor: sofawiki_project					
Product: sofawiki					
Affected Version(s): * Up to (including) 3.8.9					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	24-May-2023	9.8	SofaWiki <= 3.8.9 has a file upload vulnerability that leads to command execution. **CVE ID : CVE-2023-29721**	https://github.com/bellenuit/sofawiki/issues/27	A-SOF-SOFA-020623/473
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-May-2023	6.1	SofaWiki <=3.8.9 is vulnerable to Cross Site Scripting (XSS) via index.php. **CVE ID : CVE-2023-29720**	https://github.com/bellenuit/sofawiki/issues/26	A-SOF-SOFA-020623/474
Vendor: sqlite_jdbc_project					
Product: sqlite_jdbc					
Affected Version(s): From (including) 3.6.14.1 Up to (excluding) 3.41.2.2					
Improper Control of Generation of Code ('Code Injection')	23-May-2023	9.8	SQLite JDBC is a library for accessing and creating SQLite database files in Java. Sqlite-jdbc addresses a remote code execution vulnerability via JDBC URL. This issue impacting versions 3.6.14.1 through 3.41.2.1 and has been fixed in version 3.41.2.2. **CVE ID : CVE-2023-32697**	https://github.com/xerial/sqlite-jdbc/security/advisories/GHSA-6phf-6h5g-97j2	A-SQL-SQLI-020623/475
Vendor: squarepiginteractive					
Product: fusioninvoice					
Affected Version(s): 2023-1.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-May-2023	6.1	Stored Cross Site Scripting (XSS) vulnerability in Square Pig FusionInvoice 2023-1.0, allows attackers to execute arbitrary code via the description or content fields to the expenses, tasks, and customer details. **CVE ID : CVE-2023-25439**	N/A	A-SQU-FUSI-020623/476
Vendor: srs_simple_hits_counter_project					
Product: srs_simple_hits_counter					
Affected Version(s): * Up to (including) 1.1.0					
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Atif N SRS Simple Hits Counter plugin <= 1.1.0 versions. **CVE ID : CVE-2023-22709**	N/A	A-SRS-SRS_-020623/477
Vendor: sscms					
Product: siteserver_cms					
Affected Version(s): * Up to (including) 7.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-May-2023	6.1	A vulnerability, which was classified as problematic, was found in SiteServer CMS up to 7.2.1. Affected is an unknown function of the file /api/stl/actions/search. The manipulation of the	https://gitee.com/siteserver/cms/issues/I71WJ4	A-SSC-SITE-020623/478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument ajaxDivId leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. VDB-229818 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-2862**		
Vendor: storecommander					
Product: customers_export					
Affected Version(s): * Up to (excluding) 3.6.2					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-May-2023	9.8	In the Store Commander scexportcustomers module for PrestaShop through 3.6.1, sensitive SQL calls can be executed with a trivial HTTP request and exploited to forge a blind SQL injection. **CVE ID : CVE-2023-33278**	https://www.storecommander.com/en/addons/480-customer-export-pro.html	A-STO-CUST-020623/479
Product: quickaccounting					
Affected Version(s): * Up to (excluding) 3.7.4					
Improper Neutralization of Special	25-May-2023	9.8	In the Store Commander scquickaccounting module for	https://www.storecommander.com/en/addons/440-	A-STO-QUIC-020623/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			PrestaShop through 3.7.3, multiple sensitive SQL calls can be executed with a trivial HTTP request and exploited to forge a blind SQL injection. **CVE ID : CVE-2023-33280**	order-export-pro.html	
Product: scquickaccounting					
Affected Version(s): * Up to (excluding) 3.7.3					
N/A	16-May-2023	6.5	Insecure permissions in the ps_customer table of Prestashop scquickaccounting before v3.7.3 allows attackers to access sensitive information stored in the component. **CVE ID : CVE-2023-30281**	N/A	A-STO-SCQU-020623/481
Vendor: student_study_center_desk_management_system_project					
Product: student_study_center_desk_management_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-May-2023	9.8	Sourcecodester Student Study Center Desk Management System v1.0 admin\reports\index.php#date_from has a SQL Injection vulnerability. **CVE ID : CVE-2023-29985**	N/A	A-STU-STUD-020623/482
Vendor: studiowombat					
Product: shoppable_images					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.2.4					
Cross-Site Request Forgery (CSRF)	18-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Studio Wombat Shoppable Images plugin <= 1.2.3 versions. **CVE ID : CVE-2023-25698**	N/A	A-STU-SHOP-020623/483
Vendor: sucms_project					
Product: sucms					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-May-2023	5.4	A vulnerability was found in Sucms 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file admin_ads.php?action=add. The manipulation of the argument intro leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-229274 is the identifier assigned to this vulnerability. **CVE ID : CVE-2023-2768**	N/A	A-SUC-SUCM-020623/484
Vendor: supsystic					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: coming_soon					
Affected Version(s): * Up to (including) 1.7.10					
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Supsystic Coming Soon by Supsystic plugin <= 1.7.10 versions. **CVE ID : CVE-2023-22714**	N/A	A-SUP-COMI-020623/485
Product: contact_form					
Affected Version(s): * Up to (including) 1.7.24					
Cross-Site Request Forgery (CSRF)	17-May-2023	8.8	The Contact Form by Supsystic plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.7.24. This is due to missing or incorrect nonce validation on the AJAX action handler. This makes it possible for unauthenticated attackers to execute AJAX actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. **CVE ID : CVE-2023-2528**	N/A	A-SUP-CONT-020623/486
Vendor: symcon					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ip_symcon					
Affected Version(s): * Up to (excluding) 6.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	7.5	The web interface of Symcon IP-Symcon before 6.3 (i.e., before 2023-05-12) allows a remote attacker to read sensitive files via .. directory-traversal sequences in the URL. **CVE ID : CVE-2023-32767**	N/A	A-SYM-IP_S-020623/487
Vendor: Synology					
Product: router_manager					
Affected Version(s): From (including) 1.2 Up to (excluding) 1.2.5-8227-6					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-May-2023	9.8	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in CGI component in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows remote attackers to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2023-32956**	https://www.synology.com/en-global/security/advisory/Synology_SA_22_25	A-SYN-ROUT-020623/488
Improper Neutralization of Special Elements	16-May-2023	8.1	Improper neutralization of special elements used in an OS command ('OS	https://www.synology.com/en-global/security/advisory/Sy	A-SYN-ROUT-020623/489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Command Injection') vulnerability in DHCP Client Functionality in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows man-in-the-middle attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2023-32955**	nology_SA_22_25	
Affected Version(s): From (including) 1.3 Up to (excluding) 1.3.1-9346-3					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-May-2023	9.8	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in CGI component in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows remote attackers to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2023-32956**	https://www.synology.com/en-global/security/advisory/Synology_SA_22_25	A-SYN-ROUT-020623/490
Improper Neutralization of Special Elements used in an	16-May-2023	8.1	Improper neutralization of special elements used in an OS command ('OS Command	https://www.synology.com/en-global/security/advisory/Sy	A-SYN-ROUT-020623/491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			Injection') vulnerability in DHCP Client Functionality in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows man-in-the-middle attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2023-32955**	nology_SA_22_25	
Vendor: sysstat_project					
Product: sysstat					
Affected Version(s): * Up to (including) 12.7.2					
Integer Overflow or Wraparound	18-May-2023	7.8	sysstat through 12.7.2 allows a multiplication integer overflow in check_overflow in common.c. NOTE: this issue exists because of an incomplete fix for CVE-2022-39377. **CVE ID : CVE-2023-33204**	https://github.com/sysstat/sysstat/pull/360	A-SYS-SYSS-020623/492
Vendor: Teampass					
Product: teampass					
Affected Version(s): * Up to (excluding) 3.0.9					
Improper Control of Generation of Code ('Code Injection')	24-May-2023	8.8	Code Injection in GitHub repository nilsteampassnet/teampass prior to 3.0.9. **CVE ID : CVE-2023-2859**	https://huntr.dev/bounties/d7b8ea75-c74a-4721-89bb-12e5c80fb0ba, https://github	A-TEA-TEAM-020623/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				.com/nilsteampassnet/teampass/commit/1f51482a0c4d152ca876844212b0f8f3cb9387af	
Vendor: Teeworlds					
Product: teeworlds					
Affected Version(s): 0.7.5					
Missing Release of Memory after Effective Lifetime	23-May-2023	7.5	Teeworlds v0.7.5 was discovered to contain memory leaks. **CVE ID : CVE-2023-31517**	N/A	A-TEE-TEEW-020623/494
Use After Free	23-May-2023	5.5	A heap use-after-free in the component CDataFileReader::GetItem of teeworlds v0.7.5 allows attackers to cause a Denial of Service (DoS) via a crafted map file. **CVE ID : CVE-2023-31518**	N/A	A-TEE-TEEW-020623/495
Vendor: Telegram					
Product: telegram					
Affected Version(s): 9.3.1					
Incorrect Authorization	19-May-2023	5.5	Telegram 9.3.1 and 9.4.0 allows attackers to access restricted files, microphone ,or video recording via the DYLD_INSERT_LIBRARIES flag.	N/A	A-TEL-TELE-020623/496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-26818		
Affected Version(s): 9.4					
Incorrect Authorization	19-May-2023	5.5	Telegram 9.3.1 and 9.4.0 allows attackers to access restricted files, microphone ,or video recording via the DYLD_INSERT_LIBRARIES flag. **CVE ID : CVE-2023-26818**	N/A	A-TEL-TELE-020623/497
Vendor: teltonika					
Product: remote_management_system					
Affected Version(s): * Up to (excluding) 4.10.0					
Improper Authentication	22-May-2023	9.8	Teltonika's Remote Management System versions prior to 4.10.0 use device serial numbers and MAC addresses to identify devices from the user perspective for device claiming and from the device perspective for authentication. If an attacker obtained the serial number and MAC address of a device, they could authenticate as that device and steal communication credentials of the device. This could	N/A	A-TEL-REMO-020623/498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow an attacker to enable arbitrary command execution as root by utilizing management options within the newly registered devices. **CVE ID : CVE-2023-32347**		
Inclusion of Web Functionality from an Untrusted Source	22-May-2023	8.8	Teltonika's Remote Management System versions prior to 4.10.0 have a feature allowing users to access managed devices' local secure shell (SSH)/web management services over the cloud proxy. A user can request a web proxy and obtain a URL in the Remote Management System cloud subdomain. This URL could be shared with others without Remote Management System authentication . An attacker could exploit this vulnerability to create a malicious	N/A	A-TEL-REMO-020623/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			webpage that uses a trusted and certified domain. An attacker could initiate a reverse shell when a victim connects to the malicious webpage, achieving remote code execution on the victim device. **CVE ID : CVE-2023-2588**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-May-2023	8.3	Teltonika's Remote Management System versions prior to 4.10.0 contain a cross-site scripting (XSS) vulnerability in the main page of the web interface. An attacker with the MAC address and serial number of a connected device could send a maliciously crafted JSON file with an HTML object to trigger the vulnerability. This could allow the attacker to execute scripts in the account context and obtain remote code execution on managed devices.	N/A	A-TEL-REMO-020623/500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2587		
Observable Response Discrepancy	22-May-2023	5.3	Teltonika's Remote Management System versions prior to 4.10.0 contain a function that allows users to claim their devices. This function returns information based on whether the serial number of a device has already been claimed, the MAC address of a device has already been claimed, or whether the attempt to claim a device was successful. An attacker could exploit this to create a list of the serial numbers and MAC addresses of all devices cloud-connected to the Remote Management System. **CVE ID : CVE-2023-32346**	N/A	A-TEL-REMO-020623/501
Affected Version(s): 4.14.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	22-May-2023	9.8	Teltonika's Remote Management System versions 4.14.0 is vulnerable to an unauthorized attacker registering previously unregistered devices through the RMS platform. If the user has not disabled the "RMS management feature" enabled by default, then an attacker could register that device to themselves. This could enable the attacker to perform different operations on the user's devices, including remote code execution with 'root' privileges (using the 'Task Manager' feature on RMS). **CVE ID : CVE-2023-2586**	N/A	A-TEL-REMO-020623/502
Vendor: teslamate_project					
Product: teslamate					
Affected Version(s): 1.27.1					
Exposure of Sensitive Information to an	18-May-2023	5.3	An issue in Teslamate v1.27.1 allows attackers to obtain sensitive	N/A	A-TES-TESL-020623/503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor			information via directly accessing the teslamate link. **CVE ID : CVE-2023-29857**		
Vendor: theguidex					
Product: user_ip_and_location					
Affected Version(s): * Up to (excluding) 2.2.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in TheGuideX User IP and Location plugin <= 2.2 versions. **CVE ID : CVE-2023-30780**	N/A	A-THE-USER-020623/504
Vendor: themeisle					
Product: multiple_page_generator					
Affected Version(s): * Up to (excluding) 3.3.18					
Cross-Site Request Forgery (CSRF)	17-May-2023	4.3	The Multiple Page Generator Plugin for WordPress is vulnerable to Cross-Site Request Forgery leading to time-based SQL Injection via the orderby and order parameters in versions up to, and including, 3.3.17 due to missing nonce verification on the projects_list function and insufficient escaping on the user supplied parameter and lack	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2910686%40multiple-pages-generator-by-porthas%2Ftrunk&old=2905353%40multiple-pages-generator-by-porthas%2Ftrunk&sfp_email=&sfph_mail=	A-THE-MULT-020623/505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries leading to resource exhaustion via a forged request granted they can trick an administrator into performing an action such as clicking on a link. Version 3.3.18 addresses the SQL Injection, which drastically reduced the severity. **CVE ID : CVE-2023-2608**		
Vendor: themeist					
Product: i_recommend_this					
Affected Version(s): * Up to (including) 3.8.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Harish Chouhan, Themeist I Recommend This plugin <= 3.8.3 versions. **CVE ID : CVE-2023-23673**	N/A	A-THE-I_RE-020623/506
Vendor: theme_park_ticketing_system_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: theme_park_ticketing_system					
Affected Version(s): 1.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-May-2023	9.8	A vulnerability was found in SourceCodester Theme Park Ticketing System 1.0. It has been classified as critical. This affects an unknown part of the file print_ticket.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-229821 was assigned to this vulnerability. **CVE ID : CVE-2023-2865**	N/A	A-THE-THEM-020623/507
Vendor: theme_tweaker_project					
Product: theme_tweaker					
Affected Version(s): * Up to (including) 5.20					
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Manoj Thulasidas Theme Tweaker plugin <= 5.20 versions.	N/A	A-THE-THEM-020623/508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23713		
Vendor: thenewsletterplugin					
Product: newsletter					
Affected Version(s): * Up to (excluding) 7.6.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	6.1	Cross-site scripting vulnerability in Newsletter versions prior to 7.6.9 allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-27922**	N/A	A-THE-NEWS-020623/509
Vendor: thimpress					
Product: learnpress					
Affected Version(s): * Up to (including) 4.0.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ThimPress LearnPress Export Import plugin <= 4.0.2 versions. **CVE ID : CVE-2023-30487**	N/A	A-THI-LEAR-020623/510
Vendor: tongda2000					
Product: tongda_oa					
Affected Version(s): 11.10					
Unrestricted Upload of File with Dangerous Type	16-May-2023	9.8	A vulnerability classified as critical has been found in Tongda OA 11.10. This affects the function actionGetdata of the file	N/A	A-TON-TONG-020623/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			GatewayController.php. The manipulation leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-229149 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2738**		
Vendor: tribe29					
Product: checkmk					
Affected Version(s): 2.0.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	8.8	Improper neutralization of livestatus command delimiters in the RestAPI in Checkmk < 2.0.0p36, < 2.1.0p28, and < 2.2.0b8 (beta) allows arbitrary livestatus command execution for authorized users.	https://checkmk.com/werk/15191	A-TRI-CHEC-020623/512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31208		
Affected Version(s): * Up to (excluding) 2.0.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	8.8	Improper neutralization of livestatus command delimiters in the RestAPI in Checkmk < 2.0.0p36, < 2.1.0p28, and < 2.2.0b8 (beta) allows arbitrary livestatus command execution for authorized users. **CVE ID : CVE-2023-31208**	https://checkmk.com/werk/15191	A-TRI-CHEC-020623/513
Affected Version(s): * Up to (excluding) 2.1.0					
N/A	17-May-2023	4.3	Improper Authorization in RestAPI in Checkmk GmbH's Checkmk versions <2.1.0p28 and <2.2.0b8 allows remote authenticated users to read arbitrary host_configs. **CVE ID : CVE-2023-22348**	https://checkmk.com/werk/13982	A-TRI-CHEC-020623/514
Affected Version(s): 2.1.0					
Improper Neutralization of Special Elements used in a	17-May-2023	8.8	Improper neutralization of livestatus command delimiters in the RestAPI in	https://checkmk.com/werk/15191	A-TRI-CHEC-020623/515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Checkmk < 2.0.0p36, < 2.1.0p28, and < 2.2.0b8 (beta) allows arbitrary livestatus command execution for authorized users. **CVE ID : CVE-2023-31208**		
N/A	17-May-2023	4.3	Improper Authorization in RestAPI in Checkmk GmbH's Checkmk versions <2.1.0p28 and <2.2.0b8 allows remote authenticated users to read arbitrary host_configs. **CVE ID : CVE-2023-22348**	https://checkmk.com/werk/13982	A-TRI-CHEC-020623/516
Affected Version(s): 2.2.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	8.8	Improper neutralization of livestatus command delimiters in the RestAPI in Checkmk < 2.0.0p36, < 2.1.0p28, and < 2.2.0b8 (beta) allows arbitrary livestatus command execution for authorized users. **CVE ID : CVE-2023-31208**	https://checkmk.com/werk/15191	A-TRI-CHEC-020623/517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-May-2023	4.3	Improper Authorization in RestAPI in Checkmk GmbH's Checkmk versions <2.1.0p28 and <2.2.0b8 allows remote authenticated users to read arbitrary host_configs. **CVE ID : CVE-2023-22348**	https://checkmk.com/werk/13982	A-TRI-CHEC-020623/518
Vendor: TUG					
Product: tex_live					
Affected Version(s): From (including) 2017 Up to (excluding) 2023					
N/A	20-May-2023	7.8	LuaTeX before 1.17.0 allows execution of arbitrary shell commands when compiling a TeX file obtained from an untrusted source. This occurs because luatex-core.lua lets the original io.popen be accessed. This also affects TeX Live before 2023 r66984 and MiKTeX before 23.5. **CVE ID : CVE-2023-32700**	https://tug.org/~mseven/luatex.html	A-TUG-TEX_-020623/519
Vendor: tuzitio					
Product: camaleon_cms					
Affected Version(s): * Up to (including) 2.7.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	26-May-2023	9.8	Camaleon CMS v2.7.0 was discovered to contain a Server-Side Template Injection (SSTI) vulnerability via the formats parameter. **CVE ID : CVE-2023-30145**	N/A	A-TUZ-CAMA-020623/520
Vendor: tychesoftwares					
Product: arconix_shortcodes					
Affected Version(s): * Up to (including) 2.1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Tyche Softwares Arconix Shortcodes plugin <= 2.1.7 versions. **CVE ID : CVE-2023-23703**	N/A	A-TYC-ARCO-020623/521
Vendor: uncannyowl					
Product: uncanny_toolkit_for_learndash					
Affected Version(s): * Up to (including) 3.6.4.1					
Cross-Site Request Forgery (CSRF)	26-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Uncanny Owl Uncanny Toolkit for LearnDash plugin <= 3.6.4.1 versions. **CVE ID : CVE-2023-23714**	N/A	A-UNC-UNCA-020623/522
Vendor: upload_file_type_settings_plugin_project					
Product: upload_file_type_settings_plugin					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Sebastian Krysmanski Upload File Type Settings plugin <= 1.1 versions. **CVE ID : CVE-2023-25781**	N/A	A-UPL-UPLO-020623/523
Vendor: upress					
Product: enable_accessibility					
Affected Version(s): * Up to (including) 1.4					
Cross-Site Request Forgery (CSRF)	25-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in uPress Enable Accessibility plugin <= 1.4 versions. **CVE ID : CVE-2023-30484**	N/A	A-UPR-ENAB-020623/524
Vendor: user-meta					
Product: user_meta_manager					
Affected Version(s): * Up to (including) 3.4.9					
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in User Meta Manager plugin <= 3.4.9 versions. **CVE ID : CVE-2023-23712**	N/A	A-USE-USER-020623/525
Vendor: Valvesoftware					
Product: half-life					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	23-May-2023	7.3	A buffer overflow in the component hl.exe of Valve Half-Life up to 5433873 allows attackers to execute arbitrary code and escalate privileges by supplying crafted parameters. **CVE ID : CVE-2023-30382**	N/A	A-VAL-HALF-020623/526
Vendor: vektor-inc					
Product: vk_all_in_one_expansion_unit					
Affected Version(s): * Up to (excluding) 9.88.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Cross-site scripting vulnerability in Profile setting function of VK All in One Expansion Unit 9.88.1.0 and earlier allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-27926**	https://www.vektor-inc.co.jp/product-update/vk-blocks-exunit-xss/	A-VEK-VK_A-020623/527
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Cross-site scripting vulnerability in CTA post function of VK All in One Expansion Unit 9.88.1.0 and earlier allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-28367**	https://www.vektor-inc.co.jp/product-update/vk-blocks-exunit-xss/	A-VEK-VK_A-020623/528
Product: vk_blocks					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.53.0.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Cross-site scripting vulnerability in Tag edit function of VK Blocks 1.53.0.1 and earlier and VK Blocks Pro 1.53.0.1 and earlier allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-27923**	https://www.vektor-inc.co.jp/product-update/vk-blocks-exunit-xss/	A-VEK-VK_B-020623/529
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Cross-site scripting vulnerability in Post function of VK Blocks 1.53.0.1 and earlier and VK Blocks Pro 1.53.0.1 and earlier allows a remote authenticated attacker to inject an arbitrary script. **CVE ID : CVE-2023-27925**	https://www.vektor-inc.co.jp/product-update/vk-blocks-exunit-xss/	A-VEK-VK_B-020623/530
Vendor: vibethemes					
Product: bp_social_connect					
Affected Version(s): * Up to (including) 1.5					
Missing Authentication for Critical Function	19-May-2023	9.8	The BP Social Connect plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.5. This is due to insufficient verification on the	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2914042%40bp-social-connect%2Ftrunk&old=1904372%40bp-	A-VIB-BP_S-020623/531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user being supplied during a Facebook login through the plugin. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email. **CVE ID : CVE-2023-2704**	social-connect%2Ftrunk&sfp_email=&sfph_mail=#file6	
Vendor: videogo_project					
Product: videogo					
Affected Version(s): 6.8.1					
N/A	16-May-2023	7.5	Incorrect access control in Videogo v6.8.1 allows attackers to access images from other devices via modification of the Device Id parameter. **CVE ID : CVE-2023-31679**	N/A	A-VID-VIDE-020623/532
N/A	16-May-2023	5.3	Incorrect access control in Videogo v6.8.1 allows attackers to bind shared devices after the connection has been ended. **CVE ID : CVE-2023-31678**	N/A	A-VID-VIDE-020623/533
Vendor: vikwp					
Product: vikbooking_hotel_booking_engine_\&_pms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.6.0					
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in E4J s.R.L. VikBooking Hotel Booking Engine & PMS plugin <= 1.5.12 versions. **CVE ID : CVE-2023-25707**	N/A	A-VIK-VIKB-020623/534
Vendor: vyper_project					
Product: vyper					
Affected Version(s): * Up to (excluding) 0.3.8					
Always-Incorrect Control Flow Implementation	19-May-2023	5.3	Vyper is a pythonic Smart Contract Language for the ethereum virtual machine. In contracts with more than one regular nonpayable function, it is possible to send funds to the default function, even if the default function is marked `nonpayable`. This applies to contracts compiled with vyper versions prior to 0.3.8. This issue was fixed by the removal of the global `calldatasize` check in commit `02339dfda`. Users are advised to upgrade to version 0.3.8. Users unable to upgrade should	https://github.com/vyperlang/vyper/security/advisories/GHSA-vxmm-cwh2-q762, https://github.com/vyperlang/vyper/commit/02339dfda0f3caabad142060d511d10bfe93c520.	A-VYP-VYPE-020623/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			avoid use of nonpayable default functions. **CVE ID : CVE-2023-32675**		
Vendor: wclovers					
Product: wcfm_membership					
Affected Version(s): * Up to (including) 2.10.7					
Authorization Bypass Through User-Controlled Key	20-May-2023	9.8	The WCFM Membership – WooCommerce Memberships for Multivendor Marketplace plugin for WordPress is vulnerable to Insecure Direct Object References in versions up to, and including, 2.10.7. This is due to the plugin providing user-controlled access to objects, letting a user bypass authorization and access system resources. This makes it possible for unauthenticated attackers to change user passwords and potentially take over administrator accounts. **CVE ID : CVE-2023-2276**	https://plugins.trac.wordpress.org/changeset/2907455/, https://www.wordfence.com/threat-intel/vulnerabilities/id/42222c64-6492-4774-b5bc-8e62a1a328cf?source=cve	A-WCL-WCFM-020623/536
Vendor: wcms					
Product: wcms					
Affected Version(s): 0.3.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	22-May-2023	9.8	In Wcms 0.3.2, an attacker can send a crafted request from a vulnerable web application backend server /wcms/wex/html.php via the finish parameter and the textAreaCode parameter. It can write arbitrary strings into custom file names and upload any files, and write malicious code to execute scripts to trigger command execution. **CVE ID : CVE-2023-31689**	N/A	A-WCM-WCMS-020623/537
Vendor: weaver					
Product: e-cology					
Affected Version(s): 9.0					
Improper Restriction of XML External Entity Reference	19-May-2023	8.8	A vulnerability classified as problematic was found in Weaver e-cology up to 9.0. Affected by this vulnerability is the function RequestInfoByXml of the component API. The manipulation leads to xml external entity reference. The associated identifier of this vulnerability is	N/A	A-WEA-E-CO-020623/538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			VDB-229411. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2806**		
Product: weaver_office_automation					
Affected Version(s): 9.5					
Absolute Path Traversal	17-May-2023	7.5	A vulnerability has been found in Weaver OA up to 9.5 and classified as problematic. This vulnerability affects unknown code of the file /E-mobile/App/System/File/downfile.php. The manipulation of the argument url leads to absolute path traversal. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-229270 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	N/A	A-WEA-WEAV-020623/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2765		
Files or Directories Accessible to External Parties	17-May-2023	7.5	A vulnerability was found in Weaver OA 9.5 and classified as problematic. This issue affects some unknown processing of the file /building/backmgr/urlpage/mobileurl/configfile/jx2_config.ini. The manipulation leads to files or directories accessible. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-229271. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2766**	N/A	A-WEA-WEAV-020623/540
Vendor: webassembly					
Product: webassembly_binary_toolkit					
Affected Version(s): 1.0.32					
N/A	23-May-2023	7.5	An issue in wasm2c 1.0.32, wasm2wat	https://github.com/WebAss	A-WEB-WEBA-020623/541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.0.32, wasm-decompile 1.0.32, and wasm-validate 1.0.32 allows attackers to cause a Denial of Service (DoS) via running a crafted binary. **CVE ID : CVE-2023-31670**	embly/wabt/issues/2199	
Improper Encoding or Escaping of Output	23-May-2023	5.5	WebAssembly wat2wasm v1.0.32 allows attackers to cause a libc++abi.dylib crash by putting '@' before a quote ("). **CVE ID : CVE-2023-31669**	N/A	A-WEB-WEBA-020623/542
Vendor: webbax					
Product: customexporter					
Affected Version(s): * Up to (including) 1.7.20					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-May-2023	7.5	Prestashop customexporter <= 1.7.20 is vulnerable to Incorrect Access Control via modules/customexporter/downloads/download.php. **CVE ID : CVE-2023-30199**	https://friends-of-presta.github.io/security-advisories/modules/2023/05/16/customexporter.html	A-WEB-CUST-020623/543
Vendor: webfwd					
Product: mail_subscribe_list					
Affected Version(s): * Up to (including) 2.1.9					
Improper Neutralization of Input During	16-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in	N/A	A-WEB-MAIL-020623/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			Richard Leishman t/a Webforward Mail Subscribe List plugin <= 2.1.9 versions. **CVE ID : CVE-2023-23657**		
Vendor: Webkitgtk					
Product: webkit2gtk3					
Affected Version(s): 2.38.5-1.el8					
Use After Free	17-May-2023	8.8	A flaw was found in the WebKitGTK package. An improper input validation issue may lead to a use-after-free vulnerability. This flaw allows attackers with network access to pass specially crafted web content files, causing a denial of service or arbitrary code execution. This CVE exists because of a CVE-2023-28205 security regression for the WebKitGTK package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2203**	N/A	A-WEB-WEBK-020623/545
Affected Version(s): 2.38.5-1.el9					
Use After Free	17-May-2023	8.8	A flaw was found in the WebKitGTK	N/A	A-WEB-WEBK-020623/546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			package. An improper input validation issue may lead to a use-after-free vulnerability. This flaw allows attackers with network access to pass specially crafted web content files, causing a denial of service or arbitrary code execution. This CVE exists because of a CVE-2023-28205 security regression for the WebKitGTK package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2203**		
Vendor: wekan_project					
Product: wekan					
Affected Version(s): * Up to (including) 6.84					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-May-2023	5.4	Wekan v6.84 and earlier is vulnerable to Cross Site Scripting (XSS). An attacker with user privilege on kanban board can insert JavaScript code in in "Reaction to comment" feature. **CVE ID : CVE-2023-31779**	https://github.com/wekan/wekan/commit/47ac33d6c234359c31d9b5eae49ed3e793907279	A-WEK-WEKA-020623/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: winwar					
Product: wp_email_capture					
Affected Version(s): * Up to (excluding) 3.10					
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Winwar Media WP Email Capture plugin <= 3.9.3 versions. **CVE ID : CVE-2023-23724**	N/A	A-WIN-WP_E-020623/548
Vendor: Wireshark					
Product: wireshark					
Affected Version(s): From (including) 3.6.0 Up to (excluding) 3.6.14					
Loop with Unreachable Exit Condition ('Infinite Loop')	26-May-2023	7.5	GDSDB infinite loop in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via packet injection or crafted capture file **CVE ID : CVE-2023-2879**	https://gitlab.com/wireshark/wireshark/-/issues/19068, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2879.json, https://www.wireshark.org/security/wnpa-sec-2023-14.html	A-WIR-WIRE-020623/549
Out-of-bounds Write	26-May-2023	5.5	BLF file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file	https://gitlab.com/wireshark/wireshark/-/issues/19084, https://gitlab.com/gitlab-org/cves/-/blob/master	A-WIR-WIRE-020623/550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2854	/2023/CVE-2023-2854.json, https://www.wireshark.org/security/wnpa-sec-2023-17.html	
Out-of-bounds Write	26-May-2023	5.5	Candump log parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file **CVE ID : CVE-2023-2855**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2855.json, https://gitlab.com/wireshark/wireshark/-/issues/19062, https://www.wireshark.org/security/wnpa-sec-2023-12.html	A-WIR-WIRE-020623/551
Out-of-bounds Write	26-May-2023	5.5	VMS TCPIPtrace file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file **CVE ID : CVE-2023-2856**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2856.json, https://gitlab.com/wireshark/wireshark/-/issues/19083, https://www.wireshark.org/security/wnpa-sec-2023-16.html	A-WIR-WIRE-020623/552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-May-2023	5.5	BLF file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file **CVE ID : CVE-2023-2857**	https://gitlab.com/wireshark/wireshark/-/issues/19063, https://www.wireshark.org/security/wnpa-sec-2023-13.html, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2857.json	A-WIR-WIRE-020623/553
Out-of-bounds Write	26-May-2023	5.5	NetScaler file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file **CVE ID : CVE-2023-2858**	https://www.wireshark.org/security/wnpa-sec-2023-15.html, https://gitlab.com/wireshark/wireshark/-/issues/19081, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2858.json	A-WIR-WIRE-020623/554
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.0.6					
Loop with Unreachable Exit Condition ('Infinite Loop')	26-May-2023	7.5	GDSDB infinite loop in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via packet injection or crafted capture file	https://gitlab.com/wireshark/wireshark/-/issues/19068, https://gitlab.com/gitlab-org/cves/-	A-WIR-WIRE-020623/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2879	/blob/master/2023/CVE-2023-2879.json, https://www.wireshark.org/security/wnpa-sec-2023-14.html	
Out-of-bounds Write	26-May-2023	5.5	BLF file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file **CVE ID : CVE-2023-2854**	https://gitlab.com/wireshark/wireshark/-/issues/19084, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2854.json, https://www.wireshark.org/security/wnpa-sec-2023-17.html	A-WIR-WIRE-020623/556
Out-of-bounds Write	26-May-2023	5.5	Candump log parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file **CVE ID : CVE-2023-2855**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2855.json, https://gitlab.com/wireshark/wireshark/-/issues/19062, https://www.wireshark.org/security/wnpa-sec-2023-12.html	A-WIR-WIRE-020623/557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-May-2023	5.5	VMS TCPIPtrace file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file **CVE ID : CVE-2023-2856**	https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2856.json, https://gitlab.com/wireshark/wireshark/-/issues/19083, https://www.wireshark.org/security/wnpa-sec-2023-16.html	A-WIR-WIRE-020623/558
Out-of-bounds Write	26-May-2023	5.5	BLF file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file **CVE ID : CVE-2023-2857**	https://gitlab.com/wireshark/wireshark/-/issues/19063, https://www.wireshark.org/security/wnpa-sec-2023-13.html, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2857.json	A-WIR-WIRE-020623/559
Out-of-bounds Write	26-May-2023	5.5	NetScaler file parser crash in Wireshark 4.0.0 to 4.0.5 and 3.6.0 to 3.6.13 allows denial of service via crafted capture file **CVE ID : CVE-2023-2858**	https://www.wireshark.org/security/wnpa-sec-2023-15.html, https://gitlab.com/wireshark/wireshark/-/issues/1908	A-WIR-WIRE-020623/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				1, https://gitlab.com/gitlab-org/cves/-/blob/master/2023/CVE-2023-2858.json	
Vendor: wondershare					
Product: filmora					
Affected Version(s): 12					
Unquoted Search Path or Element	23-May-2023	7.8	Wondershare Filmora 12 (Build 12.2.1.2088) was discovered to contain an unquoted service path vulnerability via the component NativePushService. This vulnerability allows attackers to launch processes with elevated privileges. **CVE ID : CVE-2023-31747**	N/A	A-WON-FILM-020623/561
Product: mobiletrans					
Affected Version(s): 4.0.11					
Incorrect Permission Assignment for Critical Resource	24-May-2023	7.8	Insecure permissions in MobileTrans v4.0.11 allows attackers to escalate privileges to local admin via replacing the executable file. **CVE ID : CVE-2023-31748**	N/A	A-WON-MOBI-020623/562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Woocommerce					
Product: automatewoo					
Affected Version(s): * Up to (including) 4.9.40					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WooCommerce WooCommerce Follow-Up Emails (AutomateWoo) plugin <= 4.9.40 versions. **CVE ID : CVE-2023-33319**	N/A	A-WOO-AUTO-020623/563
Vendor: woocommerce_product_vendors_project					
Product: woocommerce_product_vendors					
Affected Version(s): * Up to (including) 2.1.76					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-May-2023	6.1	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WooCommerce Product Vendors plugin <= 2.1.76 versions. **CVE ID : CVE-2023-33332**	N/A	A-WOO-WOOC-020623/564
Vendor: Wordpress					
Product: wordpress					
Affected Version(s): * Up to (excluding) 4.1.38					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&s	A-WOR-WORD-020623/565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	fp_email=&sfph_mail=	
Affected Version(s): 6.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/566
Affected Version(s): From (including) 4.2 Up to (excluding) 4.2.35					
Improper Limitation	17-May-2023	6.1	WordPress Core is vulnerable to	https://core.trac.wordpress	A-WOR-WORD-020623/567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	
Affected Version(s): From (including) 4.3 Up to (excluding) 4.3.31					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Site Scripting attack. **CVE ID : CVE-2023-2745**		
Affected Version(s): From (including) 4.4 Up to (excluding) 4.4.30					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/569
Affected Version(s): From (including) 4.5 Up to (excluding) 4.5.29					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**		
Affected Version(s): From (including) 4.6 Up to (excluding) 4.6.26					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/571
Affected Version(s): From (including) 4.7 Up to (excluding) 4.7.26					
Improper Limitation of a Pathname	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to,	https://core.trac.wordpress.org/changeset?sfp_email=&	A-WOR-WORD-020623/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	
Affected Version(s): From (including) 4.8 Up to (excluding) 4.8.22					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack.	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2745		
Affected Version(s): From (including) 4.9 Up to (excluding) 4.9.23					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/574
Affected Version(s): From (including) 5.0 Up to (excluding) 5.0.19					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**		
Affected Version(s): From (including) 5.1 Up to (excluding) 5.1.16					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/576
Affected Version(s): From (including) 5.2 Up to (excluding) 5.2.18					
Improper Limitation of a Pathname to a Restricted	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang'	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old	A-WOR-WORD-020623/577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	
Affected Version(s): From (including) 5.3 Up to (excluding) 5.3.15					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack.	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2745		
Affected Version(s): From (including) 5.4 Up to (excluding) 5.4.13					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/579
Affected Version(s): From (including) 5.5 Up to (excluding) 5.5.12					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**		
Affected Version(s): From (including) 5.6 Up to (excluding) 5.6.11					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/581
Affected Version(s): From (including) 5.7 Up to (excluding) 5.7.9					
Improper Limitation of a Pathname to a Restricted	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang'	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old	A-WOR-WORD-020623/582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	
Affected Version(s): From (including) 5.8 Up to (excluding) 5.8.7					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack.	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2745		
Affected Version(s): From (including) 5.9 Up to (excluding) 5.9.6					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/584
Affected Version(s): From (including) 6.0 Up to (excluding) 6.0.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**		
Affected Version(s): From (including) 6.1 Up to (excluding) 6.1.2					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-May-2023	6.1	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack. **CVE ID : CVE-2023-2745**	https://core.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=55765%40%2F&new=55765%40%2F&sfp_email=&sfph_mail=	A-WOR-WORD-020623/586
Vendor: worksmobile					
Product: drive_explorer					
Affected Version(s): * Up to (including) 3.5.4					
Improper Control of Generation	23-May-2023	9.8	Code injection vulnerability in Drive Explorer for	N/A	A-WOR-DRIV-020623/587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			macOS versions 3.5.4 and earlier allows an attacker who can login to the client where the affected product is installed to inject arbitrary code while processing the product execution. Since a full disk access privilege is required to execute LINE WORKS Drive Explorer, the attacker may be able to read and/or write to arbitrary files without the access privileges. **CVE ID : CVE-2023-25953**		
Vendor: wp-matomo_integration_project					
Product: wp-matomo_integration					
Affected Version(s): * Up to (including) 1.0.27					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-May-2023	4.8	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in André Bräkling WP-Matomo Integration (WP-Piwik) plugin <= 1.0.27 versions. **CVE ID : CVE-2023-33211**	N/A	A-WP--WP-M-020623/588
Vendor: wpjam_basic_project					
Product: wpjam_basic					
Affected Version(s): * Up to (excluding) 6.2.1.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Denis WPJAM Basic plugin <= 6.2.1 versions. **CVE ID : CVE-2023-23709**	N/A	A-WPJ-WPJA-020623/589
Vendor: wpmanage					
Product: uji_popup					
Affected Version(s): * Up to (including) 1.4.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WPmanage Uji Popup plugin <= 1.4.3 versions. **CVE ID : CVE-2023-23641**	N/A	A-WPM-UJI_-020623/590
Vendor: wpmaspik					
Product: maspik					
Affected Version(s): * Up to (including) 0.7.8					
Cross-Site Request Forgery (CSRF)	26-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in yonifre Maspik – Spam Blacklist plugin <= 0.7.8 versions. **CVE ID : CVE-2023-24008**	N/A	A-WPM-MASP-020623/591
Vendor: wp_tabs_slides_project					
Product: wp_tabs_slides					
Affected Version(s): * Up to (including) 2.0.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Abdul Ibad WP Tabs Slides plugin <= 2.0.3 versions. **CVE ID : CVE-2023-22688**	N/A	A-WP_-WP_T-020623/592
Vendor: wp_topbar_project					
Product: wp_topbar					
Affected Version(s): * Up to (including) 5.36					
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	Cross-Site Request Forgery (CSRF) vulnerability in Bob Goetz WP-TopBar plugin <= 5.36 versions. **CVE ID : CVE-2023-23680**	N/A	A-WP_-WP_T-020623/593
Vendor: Wso2					
Product: api_manager					
Affected Version(s): * Up to (excluding) 4.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	6.1	A reflected cross-site scripting (XSS) vulnerability in /authenticationendpoint/login.do of WSO2 API Manager before 4.2.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the tenantDomain parameter. **CVE ID : CVE-2023-31664**	https://github.com/wso2/api-manager/issues?q=is%3Aissue+is%3Aclosed+label%3AComponent%2FAPIM+closed%3A2022-04-05..2023-03-11, https://github.com/wso2/product-apim/releases/tag/v4.2.0	A-WSO-API_-020623/594
Vendor: wuzhicms					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wuzhi_cms					
Affected Version(s): 3.1.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	6.1	Wuzhi CMS v3.1.2 has a storage type XSS vulnerability in the backend of the Five Finger CMS b2b system. **CVE ID : CVE-2023-31860**	N/A	A-WUZ-WUZH-020623/595
Vendor: xootix					
Product: otp_login_woocommerce_\&_gravity_forms					
Affected Version(s): * Up to (excluding) 2.3					
Improper Authentication	17-May-2023	8.1	The OTP Login Woocommerce & Gravity Forms plugin for WordPress is vulnerable to authentication bypass. This is due to the fact that when generating OTP codes for users to use in order to login via phone number, the plugin returns these codes in an AJAX response. This makes it possible for unauthenticated attackers to obtain login codes for administrators. This does require an attacker have access to the phone number configured for an account, which can be	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&old=2912731%40mobile-login-woocommerce&new=2912731%40mobile-login-woocommerce&sfp_email=&sfph_mail=	A-XOO-OTP_-020623/596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			obtained via social engineering or reconnaissance. **CVE ID : CVE-2023-2706**		
Vendor: yasm_project					
Product: yasm					
Affected Version(s): 1.3.0.55.g101bc					
N/A	17-May-2023	7.8	yasm 1.3.0.55.g101bc was discovered to contain a segmentation violation via the function do_directive at /nasm/nasm-pp.c. **CVE ID : CVE-2023-31724**	N/A	A-YAS-YASM-020623/597
N/A	17-May-2023	5.5	yasm 1.3.0.55.g101bc was discovered to contain a segmentation violation via the function expand_mmac_params at /nasm/nasm-pp.c. **CVE ID : CVE-2023-31723**	N/A	A-YAS-YASM-020623/598
Use After Free	17-May-2023	5.5	yasm 1.3.0.55.g101bc was discovered to contain a heap-use-after-free via the function expand_mmac_params at yasm/modules/pre	N/A	A-YAS-YASM-020623/599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			procs/nasm/nasm-pp.c. **CVE ID : CVE-2023-31725**		
Vendor: Yoast					
Product: yoast_seo					
Affected Version(s): * Up to (including) 14.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-May-2023	5.4	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Yoast Yoast SEO: Local plugin <= 14.9 versions. **CVE ID : CVE-2023-28785**	N/A	A-YOA-YOAS-020623/600
Vendor: Zammad					
Product: Zammad					
Affected Version(s): * Up to (excluding) 5.4.1					
Incorrect Authorization	18-May-2023	6.5	An issue in Zammad v5.4.0 allows attackers to bypass e-mail verification using an arbitrary address and manipulate the data of the generated user. Attackers are also able to gain unauthorized access to existing tickets. **CVE ID : CVE-2023-31597**	https://zammad.com/de/advisories/zaa-2023-03	A-ZAM-ZAMM-020623/601
Vendor: zlmediakit_project					
Product: zlmediakit					
Affected Version(s): 4.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-May-2023	7.5	ZLMediaKit 4.0 is vulnerable to Directory Traversal. **CVE ID : CVE-2023-31861**	N/A	A-ZLM-ZLME-020623/602
Vendor: Zulip					
Product: Zulip					
Affected Version(s): * Up to (excluding) 6.2					
Missing Authorization	19-May-2023	3.7	Zulip is an open-source team collaboration tool with unique topic-based threading. In the event that 1: `ZulipLDAPAuthBackend` and an external authentication backend (any aside of `ZulipLDAPAuthBackend` and `EmailAuthBackend`) are the only ones enabled in `AUTHENTICATION_BACKENDS` in `/etc/zulip/settings.py` and 2: The organization permissions don't require invitations to join. An attacker can create a new account in the organization with an arbitrary email address in their control that's not in	https://github.com/zulip/zulip/commit/3df1b4dd7c210c21deb6f829df19412b74573f8d	A-ZUL-ZULI-020623/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the organization's LDAP directory. The impact is limited to installations which have this specific combination of authentication backends as described above in addition to having `Invitations are required for joining this organization` organization permission disabled. This issue has been addressed in version 6.2. Users are advised to upgrade. Users unable to upgrade may enable the `Invitations are required for joining this organization` organization permission to prevent this issue. **CVE ID : CVE-2023-28623**		
Missing Authorization	19-May-2023	3.1	Zulip is an open-source team collaboration tool with unique topic-based threading. Zulip administrators can configure Zulip to limit who can add users to streams, and separately to limit who can invite	https://github.com/zulip/zulip/commit/7c2693a2c64904d1d0af8503b57763943648cbe5	A-ZUL-ZULI-020623/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			users to the organization. In Zulip Server 6.1 and below, the UI which allows a user to invite a new user also allows them to set the streams that the new user is invited to -- even if the inviting user would not have permissions to add an existing user to streams. While such a configuration is likely rare in practice, the behavior does violate security-related controls. This does not let a user invite new users to streams they cannot see, or would not be able to add users to if they had that general permission. This issue has been addressed in version 6.2. Users are advised to upgrade. Users unable to upgrade may limit sending of invitations down to users who also have the permission to add users to streams. **CVE ID : CVE-2023-32677**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Hardware					
Vendor: ABB					
Product: terra_ac_wallbox_80a					
Affected Version(s): -					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Product: terra_ac_wallbox_ce_juno					
Affected Version(s): -					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Product: terra_ac_wallbox_ce_mid					
Affected Version(s): -					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox	https://search.abb.com/library/Download.aspx?DocumentID=9AKK1	H-ABB-TERR-020623/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5.	08468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0863		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE)	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Product: terra_ac_wallbox_ce_ptb					
Affected Version(s): -					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Product: terra_ac_wallbox_ce_symbiosis					
Affected Version(s): -					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&Docu	H-ABB-TERR-020623/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**	mentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: terra_ac_wallbox_jp					
Affected Version(s): -					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Product: terra_ac_wallbox_ul32a					
Affected Version(s): -					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Product: terra_ac_wallbox_ul40					
Affected Version(s): -					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCo	H-ABB-TERR-020623/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**	de=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	H-ABB-TERR-020623/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Vendor: Belkin					
Product: f7c063					
Affected Version(s): -					
Out-of-bounds Write	18-May-2023	9.8	A stack-based buffer overflow in the ChangeFriendlyName() function of Belkin Smart Outlet V2 F7c063 firmware_2.00.11420.OWRT.PVT_SNS V2 allows attackers to cause a Denial of Service (DoS) via a crafted UPNP request. **CVE ID : CVE-2023-27217**	N/A	H-BEL-F7C0-020623/621
Vendor: birddog					
Product: 4k_quad					
Affected Version(s): -					
Use of Hard-coded Credentials	22-May-2023	9.8	Files present on firmware images could allow an attacker to gain	N/A	H-BIR-4K_Q-020623/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access as a root user using hard-coded credentials. **CVE ID : CVE-2023-2504**		
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	The affected products have a CSRF vulnerability that could allow an attacker to execute code and upload malicious files. **CVE ID : CVE-2023-2505**	N/A	H-BIR-4K_Q-020623/623
Product: a300					
Affected Version(s): -					
Use of Hard-coded Credentials	22-May-2023	9.8	Files present on firmware images could allow an attacker to gain	N/A	H-BIR-A300-020623/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access as a root user using hard-coded credentials. **CVE ID : CVE-2023-2504**		
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	The affected products have a CSRF vulnerability that could allow an attacker to execute code and upload malicious files. **CVE ID : CVE-2023-2505**	N/A	H-BIR-A300-020623/625
Product: mini					
Affected Version(s): -					
Use of Hard-coded Credentials	22-May-2023	9.8	Files present on firmware images could allow an attacker to gain	N/A	H-BIR-MINI-020623/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access as a root user using hard-coded credentials. **CVE ID : CVE-2023-2504**		
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	The affected products have a CSRF vulnerability that could allow an attacker to execute code and upload malicious files. **CVE ID : CVE-2023-2505**	N/A	H-BIR-MINI-020623/627
Product: studio_r3					
Affected Version(s): -					
Use of Hard-coded Credentials	22-May-2023	9.8	Files present on firmware images could allow an attacker to gain	N/A	H-BIR-STUD-020623/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access as a root user using hard-coded credentials. **CVE ID : CVE-2023-2504**		
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	The affected products have a CSRF vulnerability that could allow an attacker to execute code and upload malicious files. **CVE ID : CVE-2023-2505**	N/A	H-BIR-STUD-020623/629
Vendor: Cisco					
Product: business_140ac_access_point					
Affected Version(s): -					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated,	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	H-CIS-BUSI-020623/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**		
Product: business_141acm					
Affected Version(s): -					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	H-CIS-BUSI-020623/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**		
Product: business_142acm					
Affected Version(s): -					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	H-CIS-BUSI-020623/632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: business_143acm					
Affected Version(s): -					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	H-CIS-BUSI-020623/633
Product: business_145ac_access_point					
Affected Version(s): -					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-	H-CIS-BUSI-020623/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**	auth-bypass-ggnAfdZ	
Product: business_150ax_access_point					
Affected Version(s): -					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	H-CIS-BUSI-020623/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**		
Product: business_151axm					
Affected Version(s): -					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	H-CIS-BUSI-020623/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20003		
Product: business_240ac_access_point					
Affected Version(s): -					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	H-CIS-BUSI-020623/637
Product: business_250-16p-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-BUSI-020623/638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/641
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/644
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-16t-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/648
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-BUSI-020623/649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/652
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/655
Product: business_250-24fp-4g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/656
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/659
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/663
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-24fp-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/667
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/670
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_250-24p-4g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/674
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/678
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/681
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_250-24p-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/685
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/689
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-24pp-4g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/692
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-BUSI-020623/693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/696
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/700
Product: business_250-24t-4g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/703
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/707
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-24t-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/711
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/714
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/718
Product: business_250-48p-4g					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/722
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/725
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-48p-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/729
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-BUSI-020623/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/733
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/736
Product: business_250-48pp-4g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/737
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/740
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/744
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-48t-4g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/748
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/751
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_250-48t-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/755
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/759
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/762
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_250-8fp-e-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/766
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/770
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-8p-e-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/773
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-BUSI-020623/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/777
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/781
Product: business_250-8pp-d					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/784
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/788
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-8pp-e-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/792
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/795
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/799
Product: business_250-8t-d					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/803
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/806
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-8t-e-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/810
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-BUSI-020623/811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/814
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/817
Product: business_350-12np-4x					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/818
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/821
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/825
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-12xs					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/829
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/832
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_350-12xt					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/836
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/840
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/843
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_350-16fp-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/847
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/851
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-16p-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/854
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-BUSI-020623/855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/858
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/862
Product: business_350-16p-e-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/865
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/869
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-16t-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/873
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/876
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/880
Product: business_350-16t-e-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/884
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/887
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-16xts					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/891
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-BUSI-020623/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/895
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/898
Product: business_350-24fp-4g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/899
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/902
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/906
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-24fp-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/910
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/913
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_350-24mgp-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/917
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/921
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/924
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_350-24ngp-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/928
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/932
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-24p-4g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/935
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-BUSI-020623/936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/939
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/943
Product: business_350-24p-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/946
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/950
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-24s-4g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/954
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/957
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/961
Product: business_350-24t-4g					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/965
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/968
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-24t-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/972
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-BUSI-020623/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/976
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/979
Product: business_350-24xs					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/980
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/983
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/987
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-24xt					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/991
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/994
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_350-24xts					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/998
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1002
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1005
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/1006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_350-48fp-4g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1009
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/1010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1013
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-48fp-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1016
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-BUSI-020623/1017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1020
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1024
Product: business_350-48ngp-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1027
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/1028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1031
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/1032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-48p-4g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1035
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1038
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/1039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1042
Product: business_350-48p-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1046
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1049
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-48t-4g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1053
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-BUSI-020623/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1057
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1060
Product: business_350-48t-4x					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1061
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1064
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1068
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-48xt-4x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1072
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1075
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/1076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_350-8fp-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1079
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/1080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1083
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1086
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_350-8fp-e-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1090
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/1091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1094
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-8mgp-2x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1097
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-BUSI-020623/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1101
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/1102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1105
Product: business_350-8mp-2x					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1108
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/1109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1112
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-BUSI-020623/1113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-8p-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1116
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1119
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/1120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1123
Product: business_350-8p-e-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/1124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1127
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1130
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-BUSI-020623/1131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-8s-e-2g					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1134
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-BUSI-020623/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1138
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1141
Product: business_350-8t-e-2g					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1142
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1145
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/1146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1149
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-8xt					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1153
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1156
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-BUSI-020623/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-BUSI-020623/1159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf200-24					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1160
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF20-020623/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1164
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1167
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF20-020623/1168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf200-24fp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1171
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF20-020623/1172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1175
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf200-24p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1178
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SF20-020623/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1182
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF20-020623/1183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1186
Product: sf200-48					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1189
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF20-020623/1190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1193
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF20-020623/1194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf200-48p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1197
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1200
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF20-020623/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1204
Product: sf200e-24					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF20-020623/1205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1208
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1211
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF20-020623/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf200e-24p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1215
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SF20-020623/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1219
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1222
Product: sf200e-48					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1223
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1226
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF20-020623/1227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1230
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf200e-48p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1234
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1237
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF20-020623/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf200e48p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1241
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF20-020623/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1245
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF20-020623/1248
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF20-020623/1249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf250-08					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1252
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF25-020623/1253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1256
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-08hp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1259
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SF25-020623/1260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1263
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF25-020623/1264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1267
Product: sf250-10p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1270
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF25-020623/1271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1274
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF25-020623/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-18					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1278
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1281
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF25-020623/1282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1285
Product: sf250-24					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF25-020623/1286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1289
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1292
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF25-020623/1293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-24p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1296
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SF25-020623/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1300
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1303
Product: sf250-26					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1304
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1307
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF25-020623/1308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1311
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-26hp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1315
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1318
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF25-020623/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf250-26p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1322
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF25-020623/1323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1326
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1329
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF25-020623/1330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf250-48					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1333
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF25-020623/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1337
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-48hp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1340
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SF25-020623/1341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1344
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF25-020623/1345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1348
Product: sf250-50					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1351
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF25-020623/1352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1355
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF25-020623/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-50hp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1359
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1362
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF25-020623/1363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1366
Product: sf250-50p					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF25-020623/1367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1370
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1373
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF25-020623/1374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250x-24					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1377
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SF25-020623/1378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1381
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1384
Product: sf250x-24p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1385
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1388
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF25-020623/1389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1392
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250x-48					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1396
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1399
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF25-020623/1400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf250x-48p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1403
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF25-020623/1404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1407
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF25-020623/1410
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF25-020623/1411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf300-08					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1414
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF30-020623/1415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1418
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf300-24					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1421
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SF30-020623/1422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1425
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF30-020623/1426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1429
Product: sf300-24mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1432
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF30-020623/1433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1436
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF30-020623/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf300-24p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1440
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1443
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF30-020623/1444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1447
Product: sf300-24pp					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF30-020623/1448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1451
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1454
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF30-020623/1455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf300-48					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1458
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SF30-020623/1459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1462
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1465
Product: sf300-48p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1466
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1469
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF30-020623/1470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1473
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf300-48pp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1477
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1480
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF30-020623/1481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf302-08					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1484
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF30-020623/1485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1488
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1491
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF30-020623/1492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf302-08mpp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1495
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF30-020623/1496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1499
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf302-08pp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1502
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SF30-020623/1503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1506
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF30-020623/1507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF30-020623/1510
Product: sf350-08					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1513
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF35-020623/1514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1517
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF35-020623/1518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-10					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1521
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1524
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF35-020623/1525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1528
Product: sf350-10mp					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1532
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1535
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF35-020623/1536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-10p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1539
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SF35-020623/1540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1543
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1546
Product: sf350-10sfp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1547
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1550
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1554
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-20					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1558
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1561
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf350-24					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1565
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF35-020623/1566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1569
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1572
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf350-24mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1576
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF35-020623/1577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1580
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-24p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1583
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SF35-020623/1584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1587
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF35-020623/1588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1591
Product: sf350-28					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1594
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF35-020623/1595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1598
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF35-020623/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-28mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1602
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1605
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF35-020623/1606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1609
Product: sf350-28p					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1613
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1616
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF35-020623/1617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-28sfp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1620
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SF35-020623/1621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1624
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1627
Product: sf350-48					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1628
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1631
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1635
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-48mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1639
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1642
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf350-48p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1646
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF35-020623/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1650
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1653
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf350-52					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1657
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF35-020623/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1661
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-52mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1664
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SF35-020623/1665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1668
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF35-020623/1669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1672
Product: sf350-52p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1675
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF35-020623/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1679
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF35-020623/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-8mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1683
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1686
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF35-020623/1687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1690
Product: sf350-8pd					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1694
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1697
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF35-020623/1698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf352-08					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1701
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SF35-020623/1702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1705
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1708
Product: sf352-08mp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1709
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1712
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf352-08p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1720
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1723
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf355-10p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1727
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF35-020623/1728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1731
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF35-020623/1734
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF35-020623/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf500-18p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1738
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF50-020623/1739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1742
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf500-24					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1745
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SF50-020623/1746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1749
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF50-020623/1750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1753
Product: sf500-24mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1756
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF50-020623/1757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1760
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF50-020623/1761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf500-24p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1764
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1767
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF50-020623/1768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1771
Product: sf500-48					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF50-020623/1772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1775
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1778
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF50-020623/1779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf500-48mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1782
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SF50-020623/1783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1786
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1789
Product: sf500-48p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1790
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1793
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF50-020623/1794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1797
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF50-020623/1798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf550x-24					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1801
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1804
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF55-020623/1805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf550x-24mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1808
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF55-020623/1809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1812
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1815
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SF55-020623/1816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf550x-24p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1819
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF55-020623/1820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1823
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf550x-48					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1826
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SF55-020623/1827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1830
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF55-020623/1831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1834
Product: sf550x-48mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1837
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF55-020623/1838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1841
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SF55-020623/1842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf550x-48p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1845
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1848
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SF55-020623/1849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SF55-020623/1852
Product: sg200-08					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG20-020623/1853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1856
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1859
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG20-020623/1860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg200-08p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1863
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SG20-020623/1864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1867
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1870
Product: sg200-10fp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1871
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1874
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG20-020623/1875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1878
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg200-18					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1882
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1885
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG20-020623/1886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg200-26					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1889
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG20-020623/1890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1893
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1896
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG20-020623/1897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg200-26fp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1900
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG20-020623/1901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1904
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg200-26p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1907
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SG20-020623/1908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1911
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG20-020623/1912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1915
Product: sg200-50					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1918
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG20-020623/1919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1922
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG20-020623/1923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg200-50fp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1926
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1929
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG20-020623/1930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1933
Product: sg200-50p					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG20-020623/1934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1937
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1940
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG20-020623/1941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG20-020623/1942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-08					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1944
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SG25-020623/1945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1948
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1951
Product: sg250-08hp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1952
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1955
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG25-020623/1956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-10p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1963
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1966
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG25-020623/1967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg250-18					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1970
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG25-020623/1971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1974
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1977
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG25-020623/1978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg250-24					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1981
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG25-020623/1982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1985
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-24p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1988
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SG25-020623/1989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1992
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG25-020623/1993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1996
Product: sg250-26					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/1999
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG25-020623/2000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2003
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG25-020623/2004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-26hp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2007
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2010
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG25-020623/2011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2014
Product: sg250-26p					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG25-020623/2015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2018
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2021
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG25-020623/2022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-48					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2025
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SG25-020623/2026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2029
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2032
Product: sg250-48hp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2033
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2036
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG25-020623/2037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2040
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-50					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2044
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2047
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG25-020623/2048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg250-50hp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2051
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG25-020623/2052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2055
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2058
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG25-020623/2059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg250-50p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2062
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG25-020623/2063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2066
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250x-24					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2069
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SG25-020623/2070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2073
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG25-020623/2074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2077
Product: sg250x-24p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2080
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG25-020623/2081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2084
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG25-020623/2085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250x-48					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2088
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2091
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG25-020623/2092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2095
Product: sg250x-48p					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG25-020623/2096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2099
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2102
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG25-020623/2103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG25-020623/2104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-10					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2106
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SG30-020623/2107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2110
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2113
Product: sg300-10mp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2114
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2117
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG30-020623/2118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2121
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-10mpp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2125
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2128
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG30-020623/2129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg300-10p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2132
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG30-020623/2133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2136
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2139
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG30-020623/2140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg300-10pp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2143
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG30-020623/2144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2147
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-10sfp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2150
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SG30-020623/2151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2154
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG30-020623/2155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2158
Product: sg300-20					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2161
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG30-020623/2162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2165
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG30-020623/2166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-28					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2169
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2172
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG30-020623/2173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2176
Product: sg300-28mp					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG30-020623/2177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2180
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2183
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG30-020623/2184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-28p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2187
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SG30-020623/2188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2191
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2194
Product: sg300-28pp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2195
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2198
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG30-020623/2199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2202
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-28sfp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2206
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2209
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG30-020623/2210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg300-52					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2213
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG30-020623/2214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2217
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2220
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG30-020623/2221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg300-52mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2224
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG30-020623/2225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2228
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-52p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2231
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SG30-020623/2232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2235
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG30-020623/2236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG30-020623/2239
Product: sg350-10					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2242
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG35-020623/2243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2246
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG35-020623/2247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350-10mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2250
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2253
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG35-020623/2254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2257
Product: sg350-10p					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG35-020623/2258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2261
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2264
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG35-020623/2265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350-28					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2268
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SG35-020623/2269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2272
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2275
Product: sg350-28mp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2276
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2279
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG35-020623/2280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2283
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350-28p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2287
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2290
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG35-020623/2291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg350x-12pmv					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2294
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG35-020623/2295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2298
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2301
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG35-020623/2302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg350x-24					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2305
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG35-020623/2306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2309
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350x-24mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2312
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SG35-020623/2313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2316
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG35-020623/2317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2320
Product: sg350x-24p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2323
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG35-020623/2324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2327
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG35-020623/2328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350x-24pd					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2331
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2334
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG35-020623/2335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2338
Product: sg350x-24pv					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG35-020623/2339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2342
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2345
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG35-020623/2346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350x-48					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2349
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SG35-020623/2350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2353
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2356
Product: sg350x-48mp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2357
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2360
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG35-020623/2361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2364
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350x-48p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2368
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2371
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG35-020623/2372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg350x-48pv					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2375
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG35-020623/2376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2379
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2382
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG35-020623/2383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg350x-8pmd					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2386
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG35-020623/2387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2390
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350xg-24f					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2393
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SG35-020623/2394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2397
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG35-020623/2398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2401
Product: sg350xg-24t					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2404
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG35-020623/2405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2408
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG35-020623/2409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350xg-2f10					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2412
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2415
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG35-020623/2416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2419
Product: sg350xg-48t					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG35-020623/2420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2423
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2426
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG35-020623/2427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg355-10mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2430
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SG35-020623/2431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2434
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2437
Product: sg355-10p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2438
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2441
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG35-020623/2442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2445
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG35-020623/2446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500-28					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2449
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2452
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG50-020623/2453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg500-28mpp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2456
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG50-020623/2457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2460
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2463
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG50-020623/2464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg500-28p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2467
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG50-020623/2468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2471
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500-28pp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2474
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SG50-020623/2475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2478
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG50-020623/2479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2482
Product: sg500-52p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2485
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG50-020623/2486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2489
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG50-020623/2490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500-52pp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2493
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2496
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG50-020623/2497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2500
Product: sg500x-24					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG50-020623/2501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2504
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2507
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG50-020623/2508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500x-24mpp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2511
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SG50-020623/2512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2515
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2518
Product: sg500x-24p					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2519
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2522
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG50-020623/2523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2526
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500x-48					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2530
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2533
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG50-020623/2534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg500x-48mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2537
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG50-020623/2538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2541
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2544
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG50-020623/2545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg500x-48mpp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2548
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG50-020623/2549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2552
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500x-48p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2555
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SG50-020623/2556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2559
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG50-020623/2560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2563
Product: sg500x24mpp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2566
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG50-020623/2567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2570
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG50-020623/2571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500xg-8f8t					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2574
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2577
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG50-020623/2578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2581
Product: sg500xg8f8t					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG50-020623/2582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2585
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2588
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG50-020623/2589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG50-020623/2590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg550x-24					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2592
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SG55-020623/2593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2596
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2599
Product: sg550x-24mp					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2600
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2603
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG55-020623/2604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2607
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg550x-24mpp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2611
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2614
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG55-020623/2615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg550x-24p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2618
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG55-020623/2619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2622
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2625
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG55-020623/2626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg550x-48					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2629
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG55-020623/2630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2633
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg550x-48mp					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2636
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	H-CIS-SG55-020623/2637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2640
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG55-020623/2641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2644
Product: sg550x-48p					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2647
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG55-020623/2648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2651
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	H-CIS-SG55-020623/2652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg550x-48t					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2655
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2658
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG55-020623/2659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2662
Product: sg550xg-24f					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG55-020623/2663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2666
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2669
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	H-CIS-SG55-020623/2670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg550xg-24t					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2673
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	H-CIS-SG55-020623/2674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2677
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2680
Product: sg550xg-48t					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2681
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2684
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG55-020623/2685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2688
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg550xg-8f8t					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2692
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2695
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	H-CIS-SG55-020623/2696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	H-CIS-SG55-020623/2698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Vendor: contec					
Product: solarview_compact					
Affected Version(s): -					
Incorrect Default Permissions	23-May-2023	9.1	SolarView Compact <= 6.0 is vulnerable to Insecure Permissions. Any file on the server can be read or modified because texteditor.php is not restricted. **CVE ID : CVE-2023-29919**	N/A	H-CON-SOLA-020623/2699
Product: sv-cpt-mc310					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	8.8	OS command injection vulnerability in the download page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to execute an arbitrary OS command. **CVE ID : CVE-2023-27514**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	H-CON-SV-C-020623/2700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-May-2023	8.8	Buffer overflow vulnerability in the multiple setting pages of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to execute arbitrary code. **CVE ID : CVE-2023-27518**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	H-CON-SV-C-020623/2701
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	8.8	OS command injection vulnerability in the mail setting page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows remote authenticated attackers to execute an arbitrary OS command. **CVE ID : CVE-2023-27521**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarvi	H-CON-SV-C-020623/2702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ew_230508.pdf	
Use of Hard-coded Credentials	23-May-2023	7.2	Use of hard-coded credentials exists in SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10, and SV-CPT-MC310F versions prior to Ver.8.10, which may allow a remote authenticated attacker to login the affected product with an administrative privilege and perform an unintended operation. **CVE ID : CVE-2023-27512**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	H-CON-SV-C-020623/2703
N/A	23-May-2023	4.3	Improper access control vulnerability in the system date/time setting page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to alter system date/time of the affected product.	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_se	H-CON-SV-C-020623/2704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27920	curity_solarview_230508.pdf	
Product: sv-cpt-mc310f					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	8.8	OS command injection vulnerability in the download page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to execute an arbitrary OS command. **CVE ID : CVE-2023-27514**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	H-CON-SV-C-020623/2705
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-May-2023	8.8	Buffer overflow vulnerability in the multiple setting pages of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to execute arbitrary code.	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Conte	H-CON-SV-C-020623/2706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27518	c/jp/support/security-info/contec_security_solarview_230508.pdf	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	8.8	OS command injection vulnerability in the mail setting page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows remote authenticated attackers to execute an arbitrary OS command. **CVE ID : CVE-2023-27521**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	H-CON-SV-C-020623/2707
Use of Hard-coded Credentials	23-May-2023	7.2	Use of hard-coded credentials exists in SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10, and SV-CPT-MC310F versions prior to Ver.8.10, which may allow a remote authenticated attacker to login the affected product with an administrative	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-	H-CON-SV-C-020623/2708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege and perform an unintended operation. **CVE ID : CVE-2023-27512**	/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	
N/A	23-May-2023	4.3	Improper access control vulnerability in the system date/time setting page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to alter system date/time of the affected product. **CVE ID : CVE-2023-27920**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	H-CON-SV-C-020623/2709
Vendor: control4					
Product: ca-1					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	22-May-2023	9.8		N/A	H-CON-CA-1-020623/2710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware updates, resulting in code execution. **CVE ID : CVE-2023-28386**		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1	Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection. Attackers could impersonate a device and supply	N/A	H-CON-CA-1-020623/2711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web. **CVE ID : CVE-2023-31245**		
Observable Discrepancy	22-May-2023	5.3		N/A	H-CON-CA-1-020623/2712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information. **CVE ID : CVE-2023-28412**		
N/A	22-May-2023	10	Snap One OvrC cloud servers contain a route an	N/A	H-CON-CA-1-020623/2713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker can use to bypass requirements and claim devices outright. **CVE ID : CVE-2023-31241**		
Product: ca-10					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	22-May-2023	9.8		N/A	H-CON-CA-1-020623/2714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware updates, resulting in code execution. **CVE ID : CVE-2023-28386**		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1		N/A	H-CON-CA-1-020623/2715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			locations on the web. **CVE ID : CVE-2023-31245**		
Observable Discrepancy	22-May-2023	5.3	When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be	N/A	H-CON-CA-1-020623/2716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enumerated in an attack and the OvrC cloud will disclose their information. **CVE ID : CVE-2023-28412**		
N/A	22-May-2023	10	Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright.	N/A	H-CON-CA-1-020623/2717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31241		
Product: ea-1					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	22-May-2023	9.8	Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the	N/A	H-CON-EA-1-020623/2718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware updates, resulting in code execution. **CVE ID : CVE-2023-28386**		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1		N/A	H-CON-EA-1-020623/2719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31245		
Observable Discrepancy	22-May-2023	5.3	When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information.	N/A	H-CON-EA-1-020623/2720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28412		
N/A	22-May-2023	10	Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright.	N/A	H-CON-EA-1-020623/2721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31241		
Product: ea-3					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	22-May-2023	9.8	Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow	N/A	H-CON-EA-3-020623/2722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to upload arbitrary firmware updates, resulting in code execution. **CVE ID : CVE-2023-28386**		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1		N/A	H-CON-EA-3-020623/2723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31245		
Observable Discrepancy	22-May-2023	5.3	When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information.	N/A	H-CON-EA-3-020623/2724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28412		
N/A	22-May-2023	10	Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright. **CVE ID : CVE-2023-31241**	N/A	H-CON-EA-3-020623/2725
Product: ea-5					
Affected Version(s): -					
Insufficient Verification of Data	22-May-2023	9.8		N/A	H-CON-EA-5-020623/2726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware updates, resulting in code execution.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28386		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1	Devices using Snap One OvrC cloud are sent to a web address when accessing a web management	N/A	H-CON-EA-5-020623/2727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web. **CVE ID : CVE-2023-31245**		
Observable Discrepancy	22-May-2023	5.3		N/A	H-CON-EA-5-020623/2728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information. **CVE ID : CVE-2023-28412**		
N/A	22-May-2023	10		N/A	H-CON-EA-5-020623/2729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright. **CVE ID : CVE-2023-31241**		
Vendor: Dell					
Product: dss_8440					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-	H-DEL-DSS_-020623/2730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	bounds-write-vulnerability	
Product: emc_storage_nx3240					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege.	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-EMC_-020623/2731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25537		
Product: emc_storage_nx3340					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-EMC_-020623/2732
Product: emc_xc_core_6420					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to	https://www.dell.com/support/kbdoc/en-us/00021355	H-DEL-EMC_-020623/2733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	0/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	
Product: emc_xc_core_xc640					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-EMC_-020623/2734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: emc_xc_core_xc740xd					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege.	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-EMC_-020623/2735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25537		
Product: emc_xc_core_xc740xd2					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-EMC_-020623/2736
Product: emc_xc_core_xc940					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-	H-DEL-EMC_-020623/2737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	
Product: emc_xc_core_xcxr2					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-EMC_-020623/2738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: poweredge_c4140					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: poweredge_c6420					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2740
Product: poweredge_fc640					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-	H-DEL-POWE-020623/2741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	14g-server-bios-for-an-out-of-bounds-write-vulnerability	
Product: poweredge_m640					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution or escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: poweredge_mx740c					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2743
Product: poweredge_mx840c					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2744
Product: poweredge_r440					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-	H-DEL-POWE-020623/2745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	bounds-write-vulnerability	
Product: poweredge_r540					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: poweredge_r640					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2747
Product: poweredge_r740					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2748
Product: poweredge_r740xd					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-	H-DEL-POWE-020623/2749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	bounds-write-vulnerability	
Product: poweredge_r740xd2					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: poweredge_r840					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2751
Product: poweredge_r940					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2752
Product: poweredge_r940xa					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-	H-DEL-POWE-020623/2753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	bounds-write-vulnerability	
Product: poweredge_t440					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: poweredge_t640					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2755
Product: poweredge_xe2420					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2756
Product: poweredge_xe7420					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-	H-DEL-POWE-020623/2757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	bounds-write-vulnerability	
Product: poweredge_xe7440					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: poweredge_xr2					
Affected Version(s): -					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	H-DEL-POWE-020623/2759
Vendor: Dlink					
Product: dir-300					
Affected Version(s): a					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-May-2023	9.8	D-Link DIR-300 firmware <=REVA1.06 and <=REVB2.06 is vulnerable to File inclusion via /model/__lang_msg.php. **CVE ID : CVE-2023-31814**	N/A	H-DLI-DIR--020623/2760
Affected Version(s): b					
N/A	23-May-2023	9.8	D-Link DIR-300 firmware <=REVA1.06 and <=REVB2.06 is vulnerable to File inclusion via /model/__lang_msg.php. **CVE ID : CVE-2023-31814**	N/A	H-DLI-DIR--020623/2761
Product: dir-605l					
Affected Version(s): -					
Out-of-bounds Write	16-May-2023	9.8	D-Link DIR-605L firmware version 1.17B01 BETA is vulnerable to stack overflow via /goform/formTcpipSetup, **CVE ID : CVE-2023-29961**	N/A	H-DLI-DIR--020623/2762
Vendor: eparks					
Product: fiberlink_210					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-May-2023	7.2	An OS Command Injection vulnerability in Parks Fiberlink 210 firmware version	N/A	H-EPA-FIBE-020623/2763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			V2.1.14_X000 was found via the /boaform/admin/formPing target_addr parameter. **CVE ID : CVE-2023-33617**		
Vendor: especmic					
Product: rs-12n					
Affected Version(s): -					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-RS-1-020623/2764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-RS-1-020623/2765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-RS-1-020623/2766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-RS-1-020623/2767
Product: rt-12n					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-RT-1-020623/2768
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-	H-ESP-RT-1-020623/2769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**	12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-	H-ESP-RT-1-020623/2770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**	12N, https://www.tandd.com/news/detail.html?id=780	
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/ne	H-ESP-RT-1-020623/2771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**	ws/detail.html?id=780	
Product: rt-22bn					
Affected Version(s): -					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/ne	H-ESP-RT-2-020623/2772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**	ws/detail.html?id=780	
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-RT-2-020623/2773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-RT-2-020623/2774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-RT-2-020623/2775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**		
Product: teu-12n					
Affected Version(s): -					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-TEU--020623/2776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-TEU--020623/2777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-TEU--020623/2778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions).	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-ESP-TEU--020623/2779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23545		
Vendor: gira					
Product: gira_home_server					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	6.1	A vulnerability classified as problematic was found in Gira HomeServer up to 4.12.0.220829 beta. This vulnerability affects unknown code of the file /hslist. The manipulation of the argument lst with the input debug%27"><img %20src=x%20onerror=alert(document.cookie)> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-229150 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2739**	N/A	H-GIR-GIRA-020623/2780
Vendor: hanwhavision					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: ane-l6012r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANE--020623/2781
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANE--020623/2782
Product: ane-l7012r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANE--020623/2783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANE--020623/2784
Product: ano-l6012r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANO--020623/2785
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANO--020623/2786
Product: ano-l6022r					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANO--020623/2787
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANO--020623/2788
Product: ano-l6082r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANO--020623/2789
Improper Neutralization of Input	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-content/uploa	H-HAN-ANO--020623/2790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	ds/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: ano-l7012r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANO--020623/2791
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANO--020623/2792
Product: ano-l7022r					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection	https://www.hanwhavision.com/wp-content/uploads/2023/04/	H-HAN-ANO--020623/2793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANO--020623/2794
Product: ano-l7082r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANO--020623/2795
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanw	H-HAN-ANO--020623/2796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				havisionamerica.com/download/50042/	
Product: anv-l6012r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANV--020623/2797
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANV--020623/2798
Product: anv-l6023r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-ANV--020623/2799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANV--020623/2800
Product: anv-l6082r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANV--020623/2801
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANV--020623/2802
Product: anv-l7012r					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANV--020623/2803
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANV--020623/2804
Product: anv-l7082r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-ANV--020623/2805
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	H-HAN-ANV--020623/2806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: pnm-12082rvd					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2807
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2808
Product: pnm-7002vd					
Affected Version(s): -					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	H-HAN-PNM--020623/2809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2810
Product: pnm-7082rvd					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2811
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	H-HAN-PNM--020623/2812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: pnm-8082vt					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2813
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2814
Product: pnm-9000qb					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	H-HAN-PNM--020623/2815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2816
Product: pnm-9000vd					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2817
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-PNM--020623/2818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: pnm-9002vq					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2819
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2820
Product: pnm-9022v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-PNM--020623/2821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2822
Product: pnm-9031rv					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2823
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2824
Product: pnm-9084qz1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2825
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2826
Product: pnm-9084rqz					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2827
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	H-HAN-PNM--020623/2828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: pnm-9084rqz1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2829
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2830
Product: pnm-9085rqz					
Affected Version(s): -					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	H-HAN-PNM--020623/2831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2832
Product: pnm-9085rqz1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2833
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	H-HAN-PNM--020623/2834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: pnm-9322vqp					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2835
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2836
Product: pnm-c12083rvd					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	H-HAN-PNM--020623/2837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2838
Product: pnm-c7083rvd					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2839
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-PNM--020623/2840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: pnm-c9022rv					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2841
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-PNM--020623/2842
Product: qnd-6010r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QND--020623/2843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2844
Product: qnd-6011					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2845
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2846
Product: qnd-6012r					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2847
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2848
Product: qnd-6012r1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2849
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	H-HAN-QND--020623/2850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnd-6020r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2851
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2852
Product: qnd-6021					
Affected Version(s): -					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	H-HAN-QND--020623/2853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2854
Product: qnd-6022r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2855
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	H-HAN-QND--020623/2856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnd-6030r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2857
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2858
Product: qnd-6032r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	H-HAN-QND--020623/2859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2860
Product: qnd-6070r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2861
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QND--020623/2862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qnd-6082r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2863
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2864
Product: qnd-6082r1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QND--020623/2865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2866
Product: qnd-7010r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2867
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2868
Product: qnd-70142r					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2869
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2870
Product: qnd-7020r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2871
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	H-HAN-QND--020623/2872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnd-7022r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2873
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2874
Product: qnd-7030r					
Affected Version(s): -					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	H-HAN-QND--020623/2875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2876
Product: qnd-7032r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2877
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	H-HAN-QND--020623/2878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnd-7080r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2879
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2880
Product: qnd-7082r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	H-HAN-QND--020623/2881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2882
Product: qnd-8010r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2883
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QND--020623/2884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qnd-8011					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2885
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2886
Product: qnd-8020r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QND--020623/2887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2888
Product: qnd-8021					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2889
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2890
Product: qnd-8030r					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2891
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2892
Product: qnd-8080r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QND--020623/2893
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	H-HAN-QND--020623/2894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qne-7080rvw					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNE--020623/2895
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNE--020623/2896
Product: qne-7088rv					
Affected Version(s): -					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	H-HAN-QNE--020623/2897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNE--020623/2898
Product: qne-8011r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNE--020623/2899
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	H-HAN-QNE--020623/2900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qne-8021r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNE--020623/2901
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNE--020623/2902
Product: qnf-8010					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	H-HAN-QNF--020623/2903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNF--020623/2904
Product: qnf-9010					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNF--020623/2905
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QNF--020623/2906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qno-6010r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2907
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2908
Product: qno-6012r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QNO--020623/2909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2910
Product: qno-6012r1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2911
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2912
Product: qno-6020r					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2913
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2914
Product: qno-6022r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2915
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	H-HAN-QNO--020623/2916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qno-6022r1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2917
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2918
Product: qno-6030r					
Affected Version(s): -					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	H-HAN-QNO--020623/2919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2920
Product: qno-6032r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2921
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	H-HAN-QNO--020623/2922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qno-6070r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2923
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2924
Product: qno-6082r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	H-HAN-QNO--020623/2925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2926
Product: qno-6082r1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2927
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QNO--020623/2928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qno-7012r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2929
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2930
Product: qno-7020r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QNO--020623/2931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2932
Product: qno-7022r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2933
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2934
Product: qno-7030r					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2935
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2936
Product: qno-7032r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2937
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	H-HAN-QNO--020623/2938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qno-7080r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2939
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2940
Product: qno-7082r					
Affected Version(s): -					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	H-HAN-QNO--020623/2941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2942
Product: qno-8010r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2943
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	H-HAN-QNO--020623/2944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qno-8020r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2945
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2946
Product: qno-8030r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	H-HAN-QNO--020623/2947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2948
Product: qno-8080r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNO--020623/2949
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QNO--020623/2950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qnp-6230					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2951
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2952
Product: qnp-6230h					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QNP--020623/2953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2954
Product: qnp-6230rh					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2955
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2956
Product: qnp-6250					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2957
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2958
Product: qnp-6250h					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2959
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	H-HAN-QNP--020623/2960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnp-6250r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2961
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2962
Product: qnp-6320					
Affected Version(s): -					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	H-HAN-QNP--020623/2963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2964
Product: qnp-6320h					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2965
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	H-HAN-QNP--020623/2966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnp-6320hs					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2967
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2968
Product: qnp-6320r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	H-HAN-QNP--020623/2969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNP--020623/2970
Product: qnv-6010r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2971
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QNV--020623/2972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qnv-6012r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2973
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2974
Product: qnv-6012r1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QNV--020623/2975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2976
Product: qnv-6020r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2977
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2978
Product: qnv-6022r					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2979
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2980
Product: qnv-6022r1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2981
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	H-HAN-QNV--020623/2982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnv-6030r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2983
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2984
Product: qnv-6032r					
Affected Version(s): -					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	H-HAN-QNV--020623/2985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2986
Product: qnv-6070r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2987
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	H-HAN-QNV--020623/2988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnv-6082r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2989
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2990
Product: qnv-6082r1					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	H-HAN-QNV--020623/2991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2992
Product: qnv-7010r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2993
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QNV--020623/2994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qnv-7012r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2995
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2996
Product: qnv-7020r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QNV--020623/2997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2998
Product: qnv-7022r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/2999
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3000
Product: qnv-7030r					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3001
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3002
Product: qnv-7032r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3003
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	H-HAN-QNV--020623/3004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnv-7080r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3005
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3006
Product: qnv-7082r					
Affected Version(s): -					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	H-HAN-QNV--020623/3007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3008
Product: qnv-8010r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3009
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	H-HAN-QNV--020623/3010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnv-8020r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3011
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3012
Product: qnv-8030r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	H-HAN-QNV--020623/3013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3014
Product: qnv-8080r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	H-HAN-QNV--020623/3015
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	H-HAN-QNV--020623/3016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Vendor: IBM					
Product: powervm_hypervisor					
Affected Version(s): -					
Improper Input Validation	23-May-2023	7.9	IBM PowerVM Hypervisor FW860.00 through FW860.B3, FW950.00 through FW950.70, FW1010.00 through FW1010.50, FW1020.00 through FW1020.30, and FW1030.00 through FW1030.10 could allow a local attacker with control a partition that has been assigned SRIOV virtual function (VF) to cause a denial of service to a peer partition or arbitrary data corruption. IBM X-Force ID: 253175. **CVE ID : CVE-2023-30440**	https://www.ibm.com/support/pages/node/6997133, https://exchange.xforce.ibmcloud.com/vulnerabilities/253175	H-IBM-POWE-020623/3017
Product: power_system_e1050					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and	https://www.ibm.com/support/pages/node/6993021, https://excha	H-IBM-POWE-020623/3018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	nge.xforce.ibmcloud.com/vulnerabilities/252706	
Product: power_system_e1080					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**		
Product: power_system_e950					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3020
Product: power_system_e980					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered	https://www.ibm.com/supp	H-IBM-POWE-020623/3021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	ort/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	
Product: power_system_h922					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**		
Product: power_system_h924					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3023
Product: power_system_l1022					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3024
Product: power_system_l1024					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**		
Product: power_system_l922					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706.	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30438		
Product: power_system_s1014					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3027
Product: power_system_s1022					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vul	H-IBM-POWE-020623/3028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	nerabilities/252706	
Product: power_system_s1022s					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**		
Product: power_system_s1024					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3030
Product: power_system_s914					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibm	H-IBM-POWE-020623/3031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	cloud.com/vulnerabilities/252706	
Product: power_system_s922					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**		
Product: power_system_s924					
Affected Version(s): -					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	H-IBM-POWE-020623/3033
Vendor: icom					
Product: sr-7100vn					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-May-2023	6.8	Privilege escalation vulnerability in SR-7100VN firmware Ver.1.38(N) and earlier and SR-7100VN #31 firmware Ver.1.21 and earlier allows a network-adjacent attacker with administrative privilege of the affected product to obtain an administrative privilege of the OS (Operating System). As a result, an arbitrary OS command may be executed. **CVE ID : CVE-2023-28390**	https://www.icom.co.jp/news/7239/	H-ICO-SR-7-020623/3034
Product: sr-7100vn\#31					
Affected Version(s): -					
N/A	23-May-2023	6.8	Privilege escalation vulnerability in SR-7100VN firmware Ver.1.38(N) and earlier and SR-7100VN #31 firmware Ver.1.21 and earlier allows a network-adjacent attacker with administrative privilege of the affected product to obtain an administrative privilege of the OS (Operating System). As a result, an	https://www.icom.co.jp/news/7239/	H-ICO-SR-7-020623/3035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary OS command may be executed. **CVE ID : CVE-2023-28390**		
Vendor: inaba					
Product: ac-wapu-300					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	7.2	Wi-Fi AP UNIT AC-WAPU-300 v1.00_B07 and earlier, AC-WAPU-300-P v1.00_B08P and earlier, AC-WAPUM-300 v1.00_B07 and earlier, and AC-WAPUM-300-P v1.00_B08P and earlier allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-28392**	N/A	H-INA-AC-W-020623/3036
Product: ac-wapu-300-p					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	23-May-2023	7.2	Wi-Fi AP UNIT AC-WAPU-300 v1.00_B07 and earlier, AC-WAPU-300-P v1.00_B08P and earlier, AC-WAPUM-300 v1.00_B07 and earlier, and AC-WAPUM-300-P	N/A	H-INA-AC-W-020623/3037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			v1.00_B08P and earlier allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-28392**		
Product: ac-wapum-300					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	7.2	Wi-Fi AP UNIT AC-WAPU-300 v1.00_B07 and earlier, AC-WAPU-300-P v1.00_B08P and earlier, AC-WAPUM-300 v1.00_B07 and earlier, and AC-WAPUM-300-P v1.00_B08P and earlier allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-28392**	N/A	H-INA-AC-W-020623/3038
Product: ac-wapum-300-p					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-May-2023	7.2	Wi-Fi AP UNIT AC-WAPU-300 v1.00_B07 and earlier, AC-WAPU-300-P v1.00_B08P	N/A	H-INA-AC-W-020623/3039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			and earlier, AC-WAPUM-300 v1.00_B07 and earlier, and AC-WAPUM-300-P v1.00_B08P and earlier allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-28392**		
Vendor: jins					
Product: jins_meme					
Affected Version(s): -					
Use of Hard-coded Credentials	23-May-2023	6.5	JINS MEME CORE Firmware version 2.2.0 and earlier uses a hard-coded cryptographic key, which may lead to data acquired by a sensor of the affected product being decrypted by a network-adjacent attacker. **CVE ID : CVE-2023-27921**	N/A	H-JIN-JINS-020623/3040
Vendor: Linksys					
Product: e2000					
Affected Version(s): -					
Improper Neutralization of Special Elements	23-May-2023	7.2	There is a command injection vulnerability in the Linksys E2000 router with	N/A	H-LIN-E200-020623/3041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
used in a Command ('Command Injection')			firmware version 1.0.06. If an attacker gains web management privileges, they can inject commands into the post request parameters WL_atten_bb, WL_atten_radio, and WL_atten_ctl in the apply.cgi interface, thereby gaining shell privileges. **CVE ID : CVE-2023-31740**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	7.2	There is a command injection vulnerability in the Linksys E2000 router with firmware version 1.0.06. If an attacker gains web management privileges, they can inject commands into the post request parameters wl_ssid, wl_ant, wl_rate, WL_atten_ctl, ttcp_num, ttcp_size in the httpd s Start_EPI() function, thereby gaining shell privileges. **CVE ID : CVE-2023-31741**	N/A	H-LIN-E200-020623/3042
Product: wrt54gl					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-2023	7.2	There is a command injection vulnerability in the Linksys WRT54GL router with firmware version 4.30.18.006. If an attacker gains web management privileges, they can inject commands into the post request parameters wl_ant, wl_rate, WL_atten_ctl, ttcp_num, ttcp_size in the httpd s Start_EPI() function, thereby gaining shell privileges. **CVE ID : CVE-2023-31742**	N/A	H-LIN-WRT5-020623/3043
Vendor: Mitsubishielectric					
Product: melsec_ws0-geth00200					
Affected Version(s): -					
Insecure Default Initialization of Resource	19-May-2023	8.6	Active Debug Code vulnerability in Mitsubishi Electric Corporation MELSEC WS Series WS0-GETH00200 all versions allows a remote unauthenticated attacker to bypass authentication and illegally log into the affected module by connecting to it via telnet which is	https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-002_en.pdf	H-MIT-MELS-020623/3044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hidden function and is enabled by default when shipped from the factory. As a result, a remote attacker with unauthorized login can reset the module, and if certain conditions are met, he/she can disclose or tamper with the module's configuration or rewrite the firmware. **CVE ID : CVE-2023-1618**		
Vendor: nissan					
Product: sylphy_classic_2021					
Affected Version(s): -					
Authentication Bypass by Capture-replay	22-May-2023	6.5	The remote keyfob system on Nissan Sylphy Classic 2021 sends the same RF signal for each door-open request, which allows for a replay attack. **CVE ID : CVE-2023-33281**	N/A	H-NIS-SYLP-020623/3045
Vendor: qrio					
Product: q-sl2					
Affected Version(s): -					
Improper Authentication	23-May-2023	8.8	Authentication bypass vulnerability in Qrio Lock (Q-SL2) firmware version 2.0.9 and earlier allows a network-	https://qrio.me/article/announce/2023/4140/	H-QRI-Q-SL-020623/3046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to analyze the product's communication data and conduct an arbitrary operation under certain conditions. **CVE ID : CVE-2023-25946**		
Vendor: Snapone					
Product: an-110-rt-2l1w					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	22-May-2023	9.8	Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5	N/A	H-SNA-AN-1-020623/3047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware updates, resulting in code execution. **CVE ID : CVE-2023-28386**		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1		N/A	H-SNA-AN-1-020623/3048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31245		
Observable Discrepancy	22-May-2023	5.3	When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information.	N/A	H-SNA-AN-1-020623/3049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28412		
N/A	22-May-2023	10	Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright.	N/A	H-SNA-AN-1-020623/3050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31241		
Product: an-110-rt-2l1w-wifi					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	22-May-2023	9.8	Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow	N/A	H-SNA-AN-1-020623/3051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attackers to upload arbitrary firmware updates, resulting in code execution. **CVE ID : CVE-2023-28386**		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1		N/A	H-SNA-AN-1-020623/3052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31245		
Observable Discrepancy	22-May-2023	5.3	When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information.	N/A	H-SNA-AN-1-020623/3053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28412		
N/A	22-May-2023	10	Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright. **CVE ID : CVE-2023-31241**	N/A	H-SNA-AN-1-020623/3054
Product: an-310-rt-4l2w					
Affected Version(s): -					
Insufficient Verification of Data	22-May-2023	9.8		N/A	H-SNA-AN-3-020623/3055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Authenticity			Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware updates, resulting in code execution.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28386		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1	Devices using Snap One OvrC cloud are sent to a web address when accessing a web management	N/A	H-SNA-AN-3-020623/3056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web. **CVE ID : CVE-2023-31245**		
Observable Discrepancy	22-May-2023	5.3		N/A	H-SNA-AN-3-020623/3057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information. **CVE ID : CVE-2023-28412**		
N/A	22-May-2023	10		N/A	H-SNA-AN-3-020623/3058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright. **CVE ID : CVE-2023-31241**		
Product: ovrc-300-pro					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	22-May-2023	9.8		N/A	H-SNA-OVRC-020623/3059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware updates, resulting in code execution. **CVE ID : CVE-2023-28386**		
Improper Input Validation	22-May-2023	7.5	The Hub in the Snap One OvrC cloud platform is a device used to	N/A	H-SNA-OVRC-020623/3060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			centralize and manage nested devices connected to it. A vulnerability exists in which an attacker could impersonate a hub and send device requests to claim already claimed devices. The OvrC cloud platform receives the requests but does not validate if the found devices are already managed by another user. **CVE ID : CVE-2023-28649**		
N/A	22-May-2023	7.2		N/A	H-SNA-OVRC-020623/3061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			In Snap One OvrC Pro versions prior to 7.2, when logged into the superuser account, a new functionality appears that could allow users to execute arbitrary commands on the hub device.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25183		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1		N/A	H-SNA-OVRC-020623/3062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31245		
Observable Discrepancy	22-May-2023	5.3	When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC	N/A	H-SNA-OVRC-020623/3063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cloud will disclose their information. **CVE ID : CVE-2023-28412**		
N/A	22-May-2023	10	Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright.	N/A	H-SNA-OVRC-020623/3064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31241		
Product: pakedge_rk-1					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	22-May-2023	9.8	Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a	N/A	H-SNA-PAKE-020623/3065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware updates, resulting in code execution. **CVE ID : CVE-2023-28386**		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1		N/A	H-SNA-PAKE-020623/3066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31245		
Observable Discrepancy	22-May-2023	5.3	When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information.	N/A	H-SNA-PAKE-020623/3067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28412		
N/A	22-May-2023	10	Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright. **CVE ID : CVE-2023-31241**	N/A	H-SNA-PAKE-020623/3068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: pakedge_rt-3100					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	22-May-2023	9.8	Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware	N/A	H-SNA-PAKE-020623/3069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			updates, resulting in code execution. **CVE ID : CVE-2023-28386**		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1		N/A	H-SNA-PAKE-020623/3070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection. Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31245		
Observable Discrepancy	22-May-2023	5.3	When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information.	N/A	H-SNA-PAKE-020623/3071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28412		
N/A	22-May-2023	10	Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright. **CVE ID : CVE-2023-31241**	N/A	H-SNA-PAKE-020623/3072
Product: pakedge_wr-1					
Affected Version(s): -					
Insufficient Verification of Data Authenticity	22-May-2023	9.8		N/A	H-SNA-PAKE-020623/3073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snap One OvrC Pro devices versions 7.2 and prior do not validate firmware updates correctly. The device only calculates the MD5 hash of the firmware and does not check using a private-public key mechanism. The lack of complete PKI system firmware signature could allow attackers to upload arbitrary firmware updates, resulting in code execution.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28386		
URL Redirection to Untrusted Site ('Open Redirect')	22-May-2023	6.1	Devices using Snap One OvrC cloud are sent to a web address when accessing a web management interface using a HTTP connection.	N/A	H-SNA-PAKE-020623/3074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Attackers could impersonate a device and supply malicious information about the device's web server interface. By supplying malicious parameters, an attacker could redirect the user to arbitrary and dangerous locations on the web. **CVE ID : CVE-2023-31245**		
Observable Discrepancy	22-May-2023	5.3		N/A	H-SNA-PAKE-020623/3075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			When supplied with a random MAC address, Snap One OvrC cloud servers will return information about the device. The MAC address of devices can be enumerated in an attack and the OvrC cloud will disclose their information. **CVE ID : CVE-2023-28412**		
N/A	22-May-2023	10		N/A	H-SNA-PAKE-020623/3076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Snap One OvrC cloud servers contain a route an attacker can use to bypass requirements and claim devices outright. **CVE ID : CVE-2023-31241**		
Vendor: tandd					
Product: rtr-5w					
Affected Version(s): -					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-RTR--020623/3077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-RTR--020623/3078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-RTR--020623/3079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-RTR--020623/3080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**		
Product: tr-71w					
Affected Version(s): -					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-TR-7-020623/3081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-TR-7-020623/3082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions).	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-TR-7-020623/3083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-22654		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-TR-7-020623/3084
Product: tr-72w					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-TR-7-020623/3085
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC	https://www.monitoring.especmic.co.jp/post/Vulnera	H-TAN-TR-7-020623/3086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**	bilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-	H-TAN-TR-7-020623/3087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**	22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/ne	H-TAN-TR-7-020623/3088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**	ws/detail.html?id=780	
Product: wdr-3					
Affected Version(s): -					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user.	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/ne	H-TAN-WDR--020623/3089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**	ws/detail.html?id=780	
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-WDR--020623/3090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-WDR--020623/3091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-WDR--020623/3092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**		
Product: wdr-7					
Affected Version(s): -					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-WDR--020623/3093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-WDR--020623/3094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-WDR--020623/3095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-WDR--020623/3096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**		
Product: ws-2					
Affected Version(s): -					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions).	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-WS-2-020623/3097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27388		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-WS-2-020623/3098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	H-TAN-WS-2-020623/3099
Missing Authentication for	23-May-2023	5.3	Missing authentication for critical function exists in T&D	https://www.monitoring.especmic.co.jp/post/Vulnera	H-TAN-WS-2-020623/3100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**	bilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	
Vendor: Tenda					
Product: ac5					
Affected Version(s): -					
N/A	16-May-2023	9.8	Tenda AC5 router V15.03.06.28 was discovered to	https://www.tenda.com.cn/	H-TEN-AC5-020623/3101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			contain a remote code execution (RCE) vulnerability via the Mac parameter at ip/goform/WriteFacMac. **CVE ID : CVE-2023-31587**	product/AC5.html	
Vendor: totolink					
Product: a3300r					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-May-2023	9.8	TOTOLINK A3300R v17.0.0cu.557 is vulnerable to Command Injection. **CVE ID : CVE-2023-31729**	N/A	H-TOT-A330-020623/3102
Product: cp300\+					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-May-2023	9.8	A command injection vulnerability in the hostTime parameter in the function NTPSyncWithHostof TOTOLINK CP300+ V5.2cu.7594_B20200910 allows attackers to execute arbitrary commands via a crafted http packet. **CVE ID : CVE-2023-31856**	N/A	H-TOT-CP30-020623/3103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: n200re					
Affected Version(s): -					
Password in Configuration File	18-May-2023	5.5	A vulnerability classified as problematic has been found in TOTOLINK N200RE 9.3.5u.6255_B20211224. Affected is an unknown function of the file /squashfs-root/etc_ro/custom.conf of the component Telnet Service. The manipulation leads to password in configuration file. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-229374 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2790**	N/A	H-TOT-N200-020623/3104
Vendor: Tp-link					
Product: archer_vr1600v					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-May-2023	6.7	A command injection vulnerability exists in the administrative web portal in TP-Link Archer VR1600V devices running firmware Versions <= 0.1.0. 0.9.1 v5006.0 Build 220518 Rel.32480n which allows remote attackers, authenticated to the administrative web portal as an administrator user to open an operating system level shell via the 'X_TP_IfName' parameter. **CVE ID : CVE-2023-31756**	N/A	H-TP--ARCH-020623/3105
Product: tl-wpa4530_kit					
Affected Version(s): v2					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	8.8	TP-Link TL-WPA4530 KIT V2 (EU)_170406 and V2 (EU)_161115 is vulnerable to Command Injection via _httpRpmPlcDeviceAdd. **CVE ID : CVE-2023-31700**	N/A	H-TP--TL-W-020623/3106
Improper Neutralization of Special	17-May-2023	8.8	TP-Link TL-WPA4530 KIT V2 (EU)_170406 and V2 (EU)_161115 is	N/A	H-TP--TL-W-020623/3107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			vulnerable to Command Injection via _httpRpmPlcDeviceRemove. **CVE ID : CVE-2023-31701**		
Operating System					
Vendor: ABB					
Product: terra_ac_wallbox_80a_firmware					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.5.6					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Product: terra_ac_wallbox_ce_juno_firmware					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.6.6					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&Docu	O-ABB-TERR-020623/3111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**	mentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: terra_ac_wallbox_ce_mid_firmware					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.6.6					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Product: terra_ac_wallbox_ce_ptb_firmware					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.5.26					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Product: terra_ac_wallbox_ce_symbiosis_firmware					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.2.8					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCo	O-ABB-TERR-020623/3116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**	de=en&DocumentPartId=&Action=Launch	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Product: terra_ac_wallbox_jp_firmware					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.6.6					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Product: terra_ac_wallbox_ul32a_firmware					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.6.6					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&	O-ABB-TERR-020623/3121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**	Action=Launch	
Product: terra_ac_wallbox_ul40_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.5.6					
Improper Authentication	17-May-2023	8.8	Improper Authentication vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0863**		
Cleartext Transmission of Sensitive Information	17-May-2023	4.3	Cleartext Transmission of Sensitive Information vulnerability in ABB Terra AC wallbox (UL40/80A), ABB Terra AC wallbox (UL32A), ABB Terra AC wallbox (CE) (Terra AC MID), ABB Terra AC wallbox (CE) Terra AC Juno CE, ABB Terra AC wallbox (CE) Terra AC PTB, ABB Terra AC wallbox (CE) Symbiosis, ABB Terra AC wallbox (JP).This issue affects Terra AC wallbox (UL40/80A): from 1.0;0 through 1.5.5; Terra AC wallbox (UL32A) : from 1.0;0 through 1.6.5; Terra AC wallbox (CE) (Terra AC MID): from 1.0;0 through 1.6.5; Terra AC wallbox (CE) Terra AC Juno CE: from 1.0;0 through 1.6.5;	https://search.abb.com/library/Download.aspx?DocumentID=9AKK108468A1415&LanguageCode=en&DocumentPartId=&Action=Launch	O-ABB-TERR-020623/3123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Terra AC wallbox (CE) Terra AC PTB : from 1.0;0 through 1.5.25; Terra AC wallbox (CE) Symbiosis: from 1.0;0 through 1.2.7; Terra AC wallbox (JP): from 1.0;0 through 1.6.5. **CVE ID : CVE-2023-0864**		
Vendor: Apple					
Product: macos					
Affected Version(s): -					
N/A	24-May-2023	9.8	This vulnerability exposes a network port in minikube running on macOS with Docker driver that could enable unexpected remote access to the minikube container. **CVE ID : CVE-2023-1174**	N/A	O-APP-MACO-020623/3124
Vendor: Belkin					
Product: f7c063_firmware					
Affected Version(s): 2.00.11420.owrt.pvt_snsv2					
Out-of-bounds Write	18-May-2023	9.8	A stack-based buffer overflow in the ChangeFriendlyName() function of Belkin Smart Outlet V2 F7c063 firmware_2.00.114	N/A	O-BEL-F7C0-020623/3125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			20.OWRT.PVT_SNS V2 allows attackers to cause a Denial of Service (DoS) via a crafted UPNP request. **CVE ID : CVE-2023-27217**		
Vendor: birddog					
Product: 4k_quad_firmware					
Affected Version(s): 4.5.181					
Use of Hard-coded Credentials	22-May-2023	9.8	Files present on firmware images could allow an attacker to gain unauthorized access as a root user using hard-coded credentials. **CVE ID : CVE-2023-2504**	N/A	O-BIR-4K_Q-020623/3126
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	The affected products have a CSRF vulnerability that could allow an attacker to execute	N/A	O-BIR-4K_Q-020623/3127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code and upload malicious files. **CVE ID : CVE-2023-2505**		
Affected Version(s): 4.5.196					
Use of Hard-coded Credentials	22-May-2023	9.8	Files present on firmware images could allow an attacker to gain unauthorized access as a root user using hard-coded credentials. **CVE ID : CVE-2023-2504**	N/A	O-BIR-4K_Q-020623/3128
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	The affected products have a CSRF vulnerability that could allow an attacker to execute	N/A	O-BIR-4K_Q-020623/3129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code and upload malicious files. **CVE ID : CVE-2023-2505**		
Product: a300_firmware					
Affected Version(s): 3.4					
Use of Hard-coded Credentials	22-May-2023	9.8	Files present on firmware images could allow an attacker to gain unauthorized access as a root user using hard-coded credentials. **CVE ID : CVE-2023-2504**	N/A	O-BIR-A300-020623/3130
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	The affected products have a CSRF vulnerability that could allow an attacker to execute	N/A	O-BIR-A300-020623/3131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code and upload malicious files. **CVE ID : CVE-2023-2505**		
Product: mini_firmware					
Affected Version(s): 2.6.2					
Use of Hard-coded Credentials	22-May-2023	9.8	Files present on firmware images could allow an attacker to gain unauthorized access as a root user using hard-coded credentials. **CVE ID : CVE-2023-2504**	N/A	O-BIR-MINI-020623/3132
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	The affected products have a CSRF vulnerability that could allow an attacker to execute	N/A	O-BIR-MINI-020623/3133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code and upload malicious files. **CVE ID : CVE-2023-2505**		
Product: studio_r3_firmware					
Affected Version(s): 3.6.4					
Use of Hard-coded Credentials	22-May-2023	9.8	Files present on firmware images could allow an attacker to gain unauthorized access as a root user using hard-coded credentials. **CVE ID : CVE-2023-2504**	N/A	O-BIR-STUD-020623/3134
Cross-Site Request Forgery (CSRF)	22-May-2023	8.8	The affected products have a CSRF vulnerability that could allow an attacker to execute	N/A	O-BIR-STUD-020623/3135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code and upload malicious files. **CVE ID : CVE-2023-2505**		
Vendor: Cisco					
Product: business_140ac_access_point_firmware					
Affected Version(s): * Up to (excluding) 10.8.1.0					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	O-CIS-BUSI-020623/3136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20003		
Product: business_141acm_firmware					
Affected Version(s): * Up to (excluding) 10.8.1.0					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	O-CIS-BUSI-020623/3137
Product: business_142acm_firmware					
Affected Version(s): * Up to (excluding) 10.8.1.0					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-BUSI-020623/3138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**	o-sa-cbw-auth-bypass-ggnAfdZ	
Product: business_143acm_firmware					
Affected Version(s): * Up to (excluding) 10.8.1.0					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	O-CIS-BUSI-020623/3139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**		
Product: business_145ac_access_point_firmware					
Affected Version(s): * Up to (excluding) 10.8.1.0					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	O-CIS-BUSI-020623/3140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without authentication. **CVE ID : CVE-2023-20003**		
Product: business_150ax_access_point_firmware					
Affected Version(s): 10.4.2					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	O-CIS-BUSI-020623/3141
Product: business_151axm_firmware					
Affected Version(s): 10.4.2					
Missing Authentication for	18-May-2023	8.8	A vulnerability in the social login configuration	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Critical Function			option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**	enter/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	
Product: business_240ac_access_point_firmware					
Affected Version(s): * Up to (excluding) 10.8.1.0					
Missing Authentication for Critical Function	18-May-2023	8.8	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cbw-auth-bypass-ggnAfdZ	O-CIS-BUSI-020623/3143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication. **CVE ID : CVE-2023-20003**		
Product: business_250-16p-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3145
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-BUSI-020623/3146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3149
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3152
Product: business_250-16t-2g_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3153
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3156
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3160
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-24fp-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3164
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3167
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_250-24fp-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3171
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3175
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3178
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_250-24p-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3182
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3186
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-24p-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3189
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-BUSI-020623/3190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3193
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3197
Product: business_250-24pp-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3200
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3204
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3205

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-24t-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3208
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3211
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3215
Product: business_250-24t-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3219
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3222
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-48p-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3226
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-BUSI-020623/3227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3230
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3233
Product: business_250-48p-4x_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3234
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3237
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3241
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-48pp-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3245
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3248
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_250-48t-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3252
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3256
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3259
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_250-48t-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3263
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3267
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-8fp-e-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3270
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-BUSI-020623/3271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3274
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3278
Product: business_250-8p-e-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3281
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3285
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-8pp-d_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3289
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3292
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3296
Product: business_250-8pp-e-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3300
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3303
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_250-8t-d_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3307
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-BUSI-020623/3308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3311
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3314
Product: business_250-8t-e-2g_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3315
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3318
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3322
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-12np-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3326
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3327

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3329
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3331

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_350-12xs_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3333
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3337
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3338

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3340
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_350-12xt_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3344
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3348
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3349

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-16fp-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3351
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-BUSI-020623/3352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3355
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3359
Product: business_350-16p-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3360

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3362
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3366
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-16p-e-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3370
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3373
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3375

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3377
Product: business_350-16t-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3381
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3382

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3384
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-16t-e-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3388
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-BUSI-020623/3389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3392
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3393

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3395
Product: business_350-16xts_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3396
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3397

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3399
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3403
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-24fp-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3407
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3410
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3412

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_350-24fp-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3414
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3418
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3421
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_350-24mgp-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3425
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3429
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-24ngp-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3432
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-BUSI-020623/3433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3434

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3436
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3440
Product: business_350-24p-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3441

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3443
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3447
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3449

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-24p-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3451
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3454
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3458
Product: business_350-24s-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3460

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3462
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3463

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3465
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-24t-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3469
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-BUSI-020623/3470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3473
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3476
Product: business_350-24t-4x_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3477
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3478

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3480
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3484
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-24xs_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3488
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3491
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_350-24xts_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3495
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3499
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3502
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_350-24xt_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3506
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3507

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3510
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-48fp-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3513
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-BUSI-020623/3514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3515

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3517
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3521
Product: business_350-48fp-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3524
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3528
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-48ngp-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3532
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3535
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3539
Product: business_350-48p-4g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3541

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3543
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3546
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-48p-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3550
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-BUSI-020623/3551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3552

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3554
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3557
Product: business_350-48t-4g_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3558
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3561
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3565
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-48t-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3569
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3572
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_350-48xt-4x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3576
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3580
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3583
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: business_350-8fp-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3585

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3587
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3591
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-8fp-e-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3594
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-BUSI-020623/3595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3598
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3602
Product: business_350-8mgp-2x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3605
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3609
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-8mp-2x_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3613
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3616
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3620
Product: business_350-8p-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3624
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3627
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-BUSI-020623/3628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-8p-e-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3631
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-BUSI-020623/3632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3635
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3638
Product: business_350-8s-e-2g_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3639
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3642
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3646
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: business_350-8t-e-2g_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3650
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3653
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: business_350-8xt_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3657
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-BUSI-020623/3658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3661
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-BUSI-020623/3664
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-BUSI-020623/3665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf200-24fp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3668
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF20-020623/3669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3672
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf200-24p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3675
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SF20-020623/3676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3679
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF20-020623/3680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3683
Product: sf200-24_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3686
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF20-020623/3687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3690
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF20-020623/3691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf200-48p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3694
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3697
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF20-020623/3698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3699

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3701
Product: sf200-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF20-020623/3702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3705
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3708
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF20-020623/3709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf200e-24p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3712
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SF20-020623/3713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3717

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3719
Product: sf200e-24_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3720
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3723
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF20-020623/3724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3725

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3727
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf200e-48p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3731
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3734
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF20-020623/3735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf200e-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3738
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF20-020623/3739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3742
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3745
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF20-020623/3746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf200e48p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3747

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3749
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF20-020623/3750

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3753
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF20-020623/3755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-08hp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3756
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SF25-020623/3757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3758

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3760
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF25-020623/3761

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3764
Product: sf250-08_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3767
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF25-020623/3768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3769

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3771
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF25-020623/3772

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3773

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-10p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3775
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3776

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3778
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF25-020623/3779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3782
Product: sf250-18_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF25-020623/3783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3784

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3786
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3787

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3789
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF25-020623/3790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-24p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3793
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SF25-020623/3794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3795

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3797
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3800
Product: sf250-24_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3801
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3802

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3804
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF25-020623/3805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3806

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3808
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-26hp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3812
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3815
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF25-020623/3816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3817

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf250-26p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3819
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF25-020623/3820

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3823
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3826
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF25-020623/3827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf250-26_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3828

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3830
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF25-020623/3831

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3834
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-48hp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3837
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SF25-020623/3838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3841
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF25-020623/3842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3845
Product: sf250-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3846

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3848
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF25-020623/3849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3852
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF25-020623/3853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-50hp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3856
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3859
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF25-020623/3860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3861

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3863
Product: sf250-50p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF25-020623/3864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3867
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3870
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF25-020623/3871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250-50_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3874
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SF25-020623/3875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3876

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3878
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3879

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3881
Product: sf250x-24p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3882
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3885
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF25-020623/3886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3889
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf250x-24_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3893
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3894

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3896
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF25-020623/3897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf250x-48p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3900
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF25-020623/3901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3904
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3907
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF25-020623/3908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf250x-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3909

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3911
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF25-020623/3912

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3915
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF25-020623/3917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf300-08_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3918
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SF30-020623/3919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3922
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF30-020623/3923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3926
Product: sf300-24mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3927

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3929
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF30-020623/3930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3933
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF30-020623/3934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf300-24pp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3937
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3940
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF30-020623/3941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3942

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3944
Product: sf300-24p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF30-020623/3945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3948
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3951
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF30-020623/3952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf300-24_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3955
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SF30-020623/3956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3957

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3960

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3962
Product: sf300-48pp_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3963
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3966
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF30-020623/3967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3970
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf300-48p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3974
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3975

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3977
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF30-020623/3978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf300-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3981
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF30-020623/3982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3985
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3986

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3988
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF30-020623/3989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf302-08mpp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3992
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF30-020623/3993

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3996
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3997

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf302-08pp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/3999
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SF30-020623/4000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4001

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4003
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF30-020623/4004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4007
Product: sf302-08_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4010
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF30-020623/4011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4012

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4014
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF30-020623/4015

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF30-020623/4016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-08_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4018
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4019

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4021
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF35-020623/4022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4023

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4025
Product: sf350-10mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4027

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4029
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4030

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4032
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF35-020623/4033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4034

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-10p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4036
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SF35-020623/4037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4040
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4043
Product: sf350-10sfp_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4044
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4047
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4049

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4051
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-10_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4055
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4058
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf350-20_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4062
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF35-020623/4063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4066
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4069
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf350-24mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4073
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF35-020623/4074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4077
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4078

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-24p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4080
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SF35-020623/4081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4084
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF35-020623/4085

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4088
Product: sf350-24_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4089

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4091
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF35-020623/4092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4095
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF35-020623/4096

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4097

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-28mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4099
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4102
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF35-020623/4103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4106
Product: sf350-28p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4110
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4113
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF35-020623/4114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-28sfp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4117
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SF35-020623/4118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4121
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4124
Product: sf350-28_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4125
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4126

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4128
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4130

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4132
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-48mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4136
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4139
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf350-48p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4143
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF35-020623/4144

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4147
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4150
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf350-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4152

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4154
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF35-020623/4155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4158
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-52mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4161
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SF35-020623/4162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4165
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF35-020623/4166

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4169
Product: sf350-52p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4172
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF35-020623/4173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4176
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF35-020623/4177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4178

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-52_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4180
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4183
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF35-020623/4184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4187
Product: sf350-8mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4191
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4194
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF35-020623/4195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4196

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf350-8pd_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4198
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SF35-020623/4199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4200

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4202
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4203

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4205
Product: sf352-08mp_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4206
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4209
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4213
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf352-08p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4217
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4220
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf352-08_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4224
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF35-020623/4225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4228
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4231
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF35-020623/4232

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf355-10p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4235
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF35-020623/4236

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4239
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF35-020623/4241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf500-18p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4242
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SF50-020623/4243

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4246
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF50-020623/4247

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4250
Product: sf500-24mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4251

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4253
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF50-020623/4254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4256

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4257
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF50-020623/4258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf500-24p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4261
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4264
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF50-020623/4265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4268
Product: sf500-24_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF50-020623/4269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4272
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4275
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF50-020623/4276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf500-48mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4278

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4279
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SF50-020623/4280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4282

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4283
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4286
Product: sf500-48p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4287
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4290
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF50-020623/4291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4293

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4294
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4295

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf500-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4298
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4300

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4301
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF50-020623/4302

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF50-020623/4304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sf550x-24mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4305
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF55-020623/4306

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4308

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4309
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4312
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF55-020623/4313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sf550x-24p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4315

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4316
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF55-020623/4317

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4320
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4322

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf550x-24_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4323
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SF55-020623/4324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4325

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4327
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF55-020623/4328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4331
Product: sf550x-48mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4333

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4334
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF55-020623/4335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4338
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SF55-020623/4339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sf550x-48p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4342
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4343

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4344

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4345
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF55-020623/4346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4347

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4349
Product: sf550x-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SF55-020623/4350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4353
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4355

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4356
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SF55-020623/4357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SF55-020623/4358

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg200-08p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4360
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SG20-020623/4361

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4363

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4364
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4367
Product: sg200-08_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4368
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4369

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4371
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG20-020623/4372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4375
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg200-10fp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4377

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4378

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4379
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4382
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG20-020623/4383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg200-18_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4386
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG20-020623/4387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4388

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4390
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4393
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG20-020623/4394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg200-26fp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4397
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG20-020623/4398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4401
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4403

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg200-26p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4404
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SG20-020623/4405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4406

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4408
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG20-020623/4409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4412
Product: sg200-26_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4415
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG20-020623/4416

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4419
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG20-020623/4420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg200-50fp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4422

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4423
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4424

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4426
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG20-020623/4427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4430
Product: sg200-50p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG20-020623/4431

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4434
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4437
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG20-020623/4438

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg200-50_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4440

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4441
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SG20-020623/4442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4443

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4445
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG20-020623/4448
Product: sg250-08hp_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4449
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4451

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4452
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG25-020623/4453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4456
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4457

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-08_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4460
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4463
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG25-020623/4464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg250-10p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4467
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG25-020623/4468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4470

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4471
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4472

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4473

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4474
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG25-020623/4475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg250-18_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4478
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG25-020623/4479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4481

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4482
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4484

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-24p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4485
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SG25-020623/4486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4489
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG25-020623/4490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4492

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4493
Product: sg250-24_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4496
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG25-020623/4497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4498

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4500
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG25-020623/4501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-26hp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4503

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4504
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4507
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG25-020623/4508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4510

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4511
Product: sg250-26p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG25-020623/4512

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4514

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4515
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4517

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4518
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG25-020623/4519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4520

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-26_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4522
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SG25-020623/4523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4525

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4526
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4528

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4529
Product: sg250-48hp_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4530
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4532

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4533
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG25-020623/4534

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4537
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4538

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4541
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4543

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4544
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG25-020623/4545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4546

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg250-50hp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4548
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG25-020623/4549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4552
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4555
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG25-020623/4556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg250-50p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4559
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG25-020623/4560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4561

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4563
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4564

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250-50_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4566
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SG25-020623/4567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4570
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG25-020623/4571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4574
Product: sg250x-24p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4576

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4577
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG25-020623/4578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4579

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4581
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG25-020623/4582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250x-24_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4585
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4588
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG25-020623/4589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4591

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4592
Product: sg250x-48p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG25-020623/4593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4594

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4596
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4597

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4599
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG25-020623/4600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg250x-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4603
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SG25-020623/4604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4607
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG25-020623/4610
Product: sg300-10mpp_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4611
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4614
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG30-020623/4615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4618
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-10mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4622
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4625
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG30-020623/4626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg300-10pp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4629
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG30-020623/4630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4633
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4636
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG30-020623/4637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg300-10p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4640
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG30-020623/4641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4644
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-10sfp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4647
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SG30-020623/4648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4651
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG30-020623/4652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4655
Product: sg300-10_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4658
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG30-020623/4659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4662
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG30-020623/4663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-20_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4666
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4669
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG30-020623/4670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4673
Product: sg300-28mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG30-020623/4674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4675

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4677
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4678

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4680
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG30-020623/4681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-28pp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4684
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SG30-020623/4685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4687

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4688
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4690

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4691
Product: sg300-28p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4692
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4693

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4695
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG30-020623/4696

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4699
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-28sfp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4703
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4706
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG30-020623/4707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4708

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4709

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg300-28_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4710
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG30-020623/4711

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4712

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4714
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4715

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4717
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG30-020623/4718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg300-52mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4720

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4721
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG30-020623/4722

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4723

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4725
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg300-52p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4728
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SG30-020623/4729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4731

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4732
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG30-020623/4733

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4734

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4736
Product: sg300-52_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4737

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4738

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4739
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG30-020623/4740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4741

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4743
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG30-020623/4744

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG30-020623/4745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350-10mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4746

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4747
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4749

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4750
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG35-020623/4751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4752

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4753

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4754
Product: sg350-10p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG35-020623/4755

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4756

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4758
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4759

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4761
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG35-020623/4762

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350-10_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4764

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4765
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SG35-020623/4766

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4767

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4768

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4769
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4770

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4772
Product: sg350-28mp_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4773
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4775

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4776
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG35-020623/4777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4778

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4779

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4780
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4781

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350-28p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4782

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4784
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4785

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4787
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG35-020623/4788

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4790

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg350-28_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4791
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG35-020623/4792

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4793

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4794

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4795
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4797

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4798
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG35-020623/4799

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg350x-12pmv_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4800

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4801

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4802
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG35-020623/4803

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4805

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4806
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4808

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350x-24mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4809
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SG35-020623/4810

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4811

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4812

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4813
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG35-020623/4814

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4815

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4817
Product: sg350x-24pd_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4820
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG35-020623/4821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4822

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4824
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG35-020623/4825

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350x-24pv_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4828
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4831
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG35-020623/4832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4834

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4835
Product: sg350x-24p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG35-020623/4836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4837

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4839
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4840

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4842
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG35-020623/4843

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350x-24_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4846
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SG35-020623/4847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4849

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4850
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4852

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4853
Product: sg350x-48mp_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4854
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4855

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4857
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG35-020623/4858

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4861
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350x-48pv_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4864

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4865
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4867

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4868
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG35-020623/4869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4870

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg350x-48p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4872
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG35-020623/4873

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4876
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4879
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG35-020623/4880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg350x-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4882

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4883
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG35-020623/4884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4885

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4887
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4888

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350x-8pmd_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4890
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SG35-020623/4891

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4894
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG35-020623/4895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4897

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4898
Product: sg350xg-24f_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4900

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4901
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG35-020623/4902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4903

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4905
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG35-020623/4906

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350xg-24t_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4909
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4912
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG35-020623/4913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4915

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4916
Product: sg350xg-2f10_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG35-020623/4917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4918

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4920
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4921

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4923
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG35-020623/4924

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg350xg-48t_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4927
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SG35-020623/4928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4930

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4931
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4933

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4934
Product: sg355-10mp_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4935
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4936

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4938
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG35-020623/4939

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4942
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg355-10p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4945

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4946
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4948

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4949
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG35-020623/4950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4951

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG35-020623/4952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg500-28mpp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4953
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG50-020623/4954

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4957
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4960
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG50-020623/4961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg500-28pp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4963

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4964
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG50-020623/4965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4966

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4968
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4969

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500-28p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4971
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SG50-020623/4972

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4975
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG50-020623/4976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4978

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4979
Product: sg500-28_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4981

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4982
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG50-020623/4983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4984

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4986
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG50-020623/4987

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4988

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500-52pp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4989

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4990
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4991

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4992

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4993
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG50-020623/4994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4995

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4996

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4997
Product: sg500-52p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG50-020623/4998

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/4999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5000

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5001
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5002

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5003

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5004
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG50-020623/5005

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5006

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500x-24mpp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5007

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5008
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SG50-020623/5009

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5010

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5012
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5014

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5015
Product: sg500x-24p_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5016
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5017

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5018

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5019
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG50-020623/5020

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5022

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5023
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500x-24_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5025

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5027
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5028

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5030
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG50-020623/5031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5032

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg500x-48mpp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5034
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG50-020623/5035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5038
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5040

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5041
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG50-020623/5042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg500x-48mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5045
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG50-020623/5046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5049
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5051

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500x-48p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5052
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SG50-020623/5053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5056
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG50-020623/5057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5060
Product: sg500x-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5061

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5063
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG50-020623/5064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5067
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG50-020623/5068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500x24mpp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5071
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5072

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5073

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5074
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG50-020623/5075

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5076

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5078
Product: sg500xg-8f8t_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG50-020623/5079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5080

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5081

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5082
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5083

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5084

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5085
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG50-020623/5086

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg500xg8f8t_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5088

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5089
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SG50-020623/5090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5091

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5092

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5093
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5094

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG50-020623/5096
Product: sg550x-24mpp_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5097
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5099

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5100
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG55-020623/5101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5104
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5105

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg550x-24mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5107

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5108
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5109

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5111
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG55-020623/5112

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg550x-24p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5115
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG55-020623/5116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5117

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5119
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5122
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG55-020623/5123

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Product: sg550x-24_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5125

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5126
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG55-020623/5127

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5128

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5130
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg550x-48mp_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5133
Buffer Copy	18-May-2023	9.8	Multiple vulnerabilities in	https://sec.cloudapps.cisco.c	O-CIS-SG55-020623/5134

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	om/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5137
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG55-020623/5138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5139

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5141
Product: sg550x-48p_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5144
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG55-020623/5145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5146

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5148
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG55-020623/5149

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg550x-48t_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5151

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20156		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5152
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5154

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5155
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG55-020623/5156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5159
Product: sg550x-48_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG55-020623/5160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5162

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20158		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5163
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5164

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5165

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5166
Buffer Copy without	18-May-2023	9.8	Multiple vulnerabilities in the web-based user	https://sec.cloudapps.cisco.com/security/c	O-CIS-SG55-020623/5167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	enter/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5168

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg550xg-24f_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5169

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5170
Buffer Copy without Checking Size of Input	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisc	O-CIS-SG55-020623/5171

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	o-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20160		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5174
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5177
Product: sg550xg-24t_firmware					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5178
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5181
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG55-020623/5182

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5184

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20162		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5185
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**		
Product: sg550xg-48t_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5187

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5189
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5190

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5192
Buffer Copy without Checking Size of	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG55-020623/5193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5194

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-20024		
Product: sg550xg-8f8t_firmware					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20156**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5196
Buffer Copy without Checking Size of Input ('Classic	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-	O-CIS-SG55-020623/5197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20157**	multi-S9g4Nkgv	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5198

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20158**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20159**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20160**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5200
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20161**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5202

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20162**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-May-2023	9.8	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20189**	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv	O-CIS-SG55-020623/5203
Buffer Copy without Checking Size of	18-May-2023	7.5	Multiple vulnerabilities in the web-based user interface of certain Cisco Small	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurity	O-CIS-SG55-020623/5204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2023-20024**	Advisory/cisco-sa-sg-web-multi-S9g4Nkgv	
Vendor: contec					
Product: solarview_compact_firmware					
Affected Version(s): * Up to (including) 6.0					
Incorrect Default Permissions	23-May-2023	9.1	SolarView Compact <= 6.0 is vulnerable to Insecure Permissions. Any file on the server can be read or modified because texteditor.php is not restricted. **CVE ID : CVE-2023-29919**	N/A	O-CON-SOLA-020623/5205
Product: sv-cpt-mc310f_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 8.10					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	8.8	OS command injection vulnerability in the download page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to execute an arbitrary OS command. **CVE ID : CVE-2023-27514**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	O-CON-SV-C-020623/5206
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-May-2023	8.8	Buffer overflow vulnerability in the multiple setting pages of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to execute arbitrary code. **CVE ID : CVE-2023-27518**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarvi	O-CON-SV-C-020623/5207

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ew_230508.pdf	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	8.8	OS command injection vulnerability in the mail setting page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows remote authenticated attackers to execute an arbitrary OS command. **CVE ID : CVE-2023-27521**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	O-CON-SV-C-020623/5208
Use of Hard-coded Credentials	23-May-2023	7.2	Use of hard-coded credentials exists in SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10, and SV-CPT-MC310F versions prior to Ver.8.10, which may allow a remote authenticated attacker to login the affected product with an administrative privilege and perform an unintended operation.	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_se	O-CON-SV-C-020623/5209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27512	curity_solarview_230508.pdf	
N/A	23-May-2023	4.3	Improper access control vulnerability in the system date/time setting page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to alter system date/time of the affected product. **CVE ID : CVE-2023-27920**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	O-CON-SV-C-020623/5210
Product: sv-cpt-mc310_firmware					
Affected Version(s): * Up to (excluding) 8.10					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	8.8	OS command injection vulnerability in the download page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to execute	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Conte	O-CON-SV-C-020623/5211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an arbitrary OS command. **CVE ID : CVE-2023-27514**	c/jp/support/security-info/contec_security_solarview_230508.pdf	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-May-2023	8.8	Buffer overflow vulnerability in the multiple setting pages of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated attacker to execute arbitrary code. **CVE ID : CVE-2023-27518**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	O-CON-SV-C-020623/5212
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	8.8	OS command injection vulnerability in the mail setting page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows remote authenticated attackers to execute	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-	O-CON-SV-C-020623/5213

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an arbitrary OS command. **CVE ID : CVE-2023-27521**	/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	
Use of Hard-coded Credentials	23-May-2023	7.2	Use of hard-coded credentials exists in SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10, and SV-CPT-MC310F versions prior to Ver.8.10, which may allow a remote authenticated attacker to login the affected product with an administrative privilege and perform an unintended operation. **CVE ID : CVE-2023-27512**	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	O-CON-SV-C-020623/5214
N/A	23-May-2023	4.3	Improper access control vulnerability in the system date/time setting page of SolarView Compact SV-CPT-MC310 versions prior to Ver.8.10 and SV-CPT-MC310F versions prior to Ver.8.10 allows a remote authenticated	https://www.contec.com/jp/download/donwload-list/?itemid=b28c8b7c-9f40-40b2-843c-b5b04c035b0e#firmware, https://www.contec.com/jp/api/downloadlogger?down	O-CON-SV-C-020623/5215

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to alter system date/time of the affected product. **CVE ID : CVE-2023-27920**	load=/-/media/Contec/jp/support/security-info/contec_security_solarview_230508.pdf	
Vendor: Debian					
Product: debian_linux					
Affected Version(s): 10.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-May-2023	8.8	cups-filters contains backends, filters, and other software required to get the cups printing service working on operating systems other than macos. If you use the Backend Error Handler (beh) to create an accessible network printer, this security vulnerability can cause remote code execution. `beh.c` contains the line `retval = system(cmdline) >> 8;` which calls the `system` command with the operand `cmdline`. `cmdline` contains multiple user controlled, unsanitized values. As a result an attacker with network access to the hosted print	https://github.com/OpenPrinting/cups-filters/security/advisories/GHSA-gpxc-v2m8-fr3x, https://github.com/OpenPrinting/cups-filters/commit/8f27403575 6c04efeb77eb 654e9d4c444 7287d65	O-DEB-DEBI-020623/5216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			server can exploit this vulnerability to inject system commands which are executed in the context of the running server. This issue has been addressed in commit `8f2740357` and is expected to be bundled in the next release. Users are advised to upgrade when possible and to restrict access to network printers in the meantime. **CVE ID : CVE-2023-24805**		
Affected Version(s): 11.0					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-May-2023	8.8	cups-filters contains backends, filters, and other software required to get the cups printing service working on operating systems other than macos. If you use the Backend Error Handler (beh) to create an accessible network printer, this security vulnerability can cause remote code execution. `beh.c` contains the line `retval = system(cmdline) >>	https://github.com/OpenPrinting/cups-filters/security/advisories/GHSA-gpxc-v2m8-fr3x, https://github.com/OpenPrinting/cups-filters/commit/8f274035756c04efeb77eb654e9d4c4447287d65	O-DEB-DEBI-020623/5217

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			8;` which calls the `system` command with the operand `cmdline`. `cmdline` contains multiple user controlled, unsanitized values. As a result an attacker with network access to the hosted print server can exploit this vulnerability to inject system commands which are executed in the context of the running server. This issue has been addressed in commit `8f2740357` and is expected to be bundled in the next release. Users are advised to upgrade when possible and to restrict access to network printers in the meantime. **CVE ID : CVE-2023-24805**		
Use After Free	16-May-2023	8.8	Use after free in Navigation in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium	N/A	O-DEB-DEBI-020623/5218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: Critical) **CVE ID : CVE-2023-2721**		
Use After Free	16-May-2023	8.8	Use after free in Autofill UI in Google Chrome on Android prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2722**	N/A	O-DEB-DEBI-020623/5219
Use After Free	16-May-2023	8.8	Use after free in DevTools in Google Chrome prior to 113.0.5672.126 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2723**	N/A	O-DEB-DEBI-020623/5220
Access of Resource Using Incompatible Type ('Type Confusion')	16-May-2023	8.8	Type confusion in V8 in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit	N/A	O-DEB-DEBI-020623/5221

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2724**		
Use After Free	16-May-2023	8.8	Use after free in Guest View in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2725**	N/A	O-DEB-DEBI-020623/5222
N/A	16-May-2023	8.8	Inappropriate implementation in WebApp Installs in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious web app to bypass install dialog via a crafted HTML page. (Chromium security severity: Medium)	N/A	O-DEB-DEBI-020623/5223

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2726		
Vendor: Dell					
Product: dss_8440_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-DSS_-020623/5224
Product: emc_storage_nx3240_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-	O-DEL-EMC_-020623/5225

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	
Product: emc_storage_nx3340_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-EMC_-020623/5226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: emc_xc_core_6420_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege.	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-EMC_-020623/5227

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-25537		
Product: emc_xc_core_xc640_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-EMC_-020623/5228
Product: emc_xc_core_xc740xd2_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-	O-DEL-EMC_-020623/5229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	
Product: emc_xc_core_xc740xd_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-EMC_-020623/5230

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: emc_xc_core_xc940_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-EMC_-020623/5231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: emc_xc_core_xcxr2_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-EMC_-020623/5232
Product: poweredge_c4140_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-	O-DEL-POWE-020623/5233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	14g-server-bios-for-an-out-of-bounds-write-vulnerability	
Product: poweredge_c6420_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5234

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution or escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: poweredge_fc640_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5235
Product: poweredge_m640_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5236
Product: poweredge_mx740c_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-	O-DEL-POWE-020623/5237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	bounds-write-vulnerability	
Product: poweredge_mx840c_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: poweredge_r440_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5239
Product: poweredge_r540_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5240
Product: poweredge_r640_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-	O-DEL-POWE-020623/5241

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	bounds-write-vulnerability	
Product: poweredge_r740xd2_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: poweredge_r740xd_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5243
Product: poweredge_r740_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5244
Product: poweredge_r840_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-	O-DEL-POWE-020623/5245

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	bounds-write-vulnerability	
Product: poweredge_r940xa_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: poweredge_r940_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5247
Product: poweredge_t440_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5248
Product: poweredge_t640_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-	O-DEL-POWE-020623/5249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	bounds-write-vulnerability	
Product: poweredge_xe2420_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege. **CVE ID : CVE-2023-25537**		
Product: poweredge_xe7420_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5251
Product: poweredge_xe7440_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-bounds-write-vulnerability	O-DEL-POWE-020623/5252
Product: poweredge_xr2_firmware					
Affected Version(s): * Up to (excluding) 2.18.1					
Out-of-bounds Write	22-May-2023	7.8	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker	https://www.dell.com/support/kbdoc/en-us/000213550/dsa-2023-098-security-update-for-dell-poweredge-14g-server-bios-for-an-out-of-	O-DEL-POWE-020623/5253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege. **CVE ID : CVE-2023-25537**	bounds-write-vulnerability	
Vendor: Dlink					
Product: dir-300_firmware					
Affected Version(s): * Up to (including) 1.06					
N/A	23-May-2023	9.8	D-Link DIR-300 firmware <=REVA1.06 and <=REVB2.06 is vulnerable to File inclusion via /model/__lang_msg.php. **CVE ID : CVE-2023-31814**	N/A	O-DLI-DIR--020623/5254
Affected Version(s): * Up to (including) 2.06					
N/A	23-May-2023	9.8	D-Link DIR-300 firmware <=REVA1.06 and <=REVB2.06 is vulnerable to File inclusion via /model/__lang_msg.php.	N/A	O-DLI-DIR--020623/5255

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31814		
Product: dir-605l_firmware					
Affected Version(s): 1.17b01					
Out-of-bounds Write	16-May-2023	9.8	D-Link DIR-605L firmware version 1.17B01 BETA is vulnerable to stack overflow via /goform/formTcpipSetup, **CVE ID : CVE-2023-29961**	N/A	O-DLI-DIR--020623/5256
Vendor: eparks					
Product: fiberlink_210_firmware					
Affected Version(s): 2.1.14_x000					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	7.2	An OS Command Injection vulnerability in Parks Fiberlink 210 firmware version V2.1.14_X000 was found via the /boaform/admin/formPing target_addr parameter. **CVE ID : CVE-2023-33617**	N/A	O-EPA-FIBE-020623/5257
Vendor: especmic					
Product: rs-12n_firmware					
Affected Version(s): *					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-	O-ESP-RS-1-020623/5258

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**	22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/ne	O-ESP-RS-1-020623/5259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**	ws/detail.html?id=780	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-ESP-RS-1-020623/5260

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-ESP-RS-1-020623/5261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**		
Product: rt-12n_firmware					
Affected Version(s): *					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-ESP-RT-1-020623/5262

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-ESP-RT-1-020623/5263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions),	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-ESP-RT-1-020623/5264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-ESP-RT-1-020623/5265

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**		
Product: rt-22bn_firmware					
Affected Version(s): *					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-ESP-RT-2-020623/5266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions).	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-ESP-RT-2-020623/5267

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27387		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-ESP-RT-2-020623/5268
Missing Authentica	23-May-2023	5.3	Missing authentication for	https://www.monitoring.es	O-ESP-RT-2-020623/5269

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion for Critical Function			critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**	pecmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	
Product: teu-12n_firmware					
Affected Version(s): *					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-ESP-TEU--020623/5270
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-	O-ESP-TEU--020623/5271

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**	12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-	O-ESP-TEU--020623/5272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**	12N, https://www.tandd.com/news/detail.html?id=780	
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/ne	O-ESP-TEU--020623/5273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**	ws/detail.html?id=780	
Vendor: Fedoraproject					
Product: fedora					
Affected Version(s): 37					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-May-2023	8.8	cups-filters contains backends, filters, and other software required to get the cups printing service working on operating systems other than macos. If you use the Backend Error	https://github.com/OpenPrinting/cups-filters/security/advisories/GHSA-gpxc-v2m8-fr3x, https://github.com/OpenPrinting/cups-filters/commit	O-FED-FEDO-020623/5274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Handler (beh) to create an accessible network printer, this security vulnerability can cause remote code execution. `beh.c` contains the line `retval = system(cmdline) >> 8;` which calls the `system` command with the operand `cmdline`. `cmdline` contains multiple user controlled, unsanitized values. As a result an attacker with network access to the hosted print server can exploit this vulnerability to inject system commands which are executed in the context of the running server. This issue has been addressed in commit `8f2740357` and is expected to be bundled in the next release. Users are advised to upgrade when possible and to restrict access to network printers in the meantime. **CVE ID : CVE-2023-24805**	/8f274035756c04efeb77eb654e9d4c4447287d65	

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use After Free	16-May-2023	8.8	Use after free in Navigation in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) **CVE ID : CVE-2023-2721**	N/A	O-FED-FEDO-020623/5275
Use After Free	16-May-2023	8.8	Use after free in Autofill UI in Google Chrome on Android prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2722**	N/A	O-FED-FEDO-020623/5276
Use After Free	16-May-2023	8.8	Use after free in DevTools in Google Chrome prior to 113.0.5672.126 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium	N/A	O-FED-FEDO-020623/5277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			security severity: High) **CVE ID : CVE-2023-2723**		
Access of Resource Using Incompatible Type ('Type Confusion')	16-May-2023	8.8	Type confusion in V8 in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2724**	N/A	O-FED-FEDO-020623/5278
Use After Free	16-May-2023	8.8	Use after free in Guest View in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2725**	N/A	O-FED-FEDO-020623/5279
N/A	16-May-2023	8.8	Inappropriate implementation in WebApp Installs in Google Chrome prior to 113.0.5672.126	N/A	O-FED-FEDO-020623/5280

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed an attacker who convinced a user to install a malicious web app to bypass install dialog via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2726**		
Affected Version(s): 38					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-May-2023	8.8	cups-filters contains backends, filters, and other software required to get the cups printing service working on operating systems other than macos. If you use the Backend Error Handler (beh) to create an accessible network printer, this security vulnerability can cause remote code execution. `beh.c` contains the line `retval = system(cmdline) >> 8;` which calls the `system` command with the operand `cmdline`. `cmdline` contains multiple user controlled, unsanitized values. As a result an attacker with	https://github.com/OpenPrinting/cups-filters/security/advisories/GHSA-gpxc-v2m8-fr3x, https://github.com/OpenPrinting/cups-filters/commit/8f274035756c04efeb77eb654e9d4c4447287d65	O-FED-FEDO-020623/5281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network access to the hosted print server can exploit this vulnerability to inject system commands which are executed in the context of the running server. This issue has been addressed in commit `8f2740357` and is expected to be bundled in the next release. Users are advised to upgrade when possible and to restrict access to network printers in the meantime. **CVE ID : CVE-2023-24805**		
Use After Free	16-May-2023	8.8	Use after free in Navigation in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical) **CVE ID : CVE-2023-2721**	N/A	O-FED-FEDO-020623/5282
Use After Free	16-May-2023	8.8	Use after free in Autofill UI in Google Chrome on Android prior to 113.0.5672.126	N/A	O-FED-FEDO-020623/5283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2722**		
Use After Free	16-May-2023	8.8	Use after free in DevTools in Google Chrome prior to 113.0.5672.126 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2723**	N/A	O-FED-FEDO-020623/5284
Access of Resource Using Incompatible Type ('Type Confusion')	16-May-2023	8.8	Type confusion in V8 in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2724**	N/A	O-FED-FEDO-020623/5285
Use After Free	16-May-2023	8.8	Use after free in Guest View in	N/A	O-FED-FEDO-020623/5286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2725**		
N/A	16-May-2023	8.8	Inappropriate implementation in WebApp Installs in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious web app to bypass install dialog via a crafted HTML page. (Chromium security severity: Medium) **CVE ID : CVE-2023-2726**	N/A	O-FED-FEDO-020623/5287
NULL Pointer Dereference	17-May-2023	5.5	A NULL pointer dereference flaw was found in Libtiff's LZWDecode() function in the libtiff/tif_lzw.c file. This flaw allows a local attacker to	https://github.com/libsdl-org/libtiff/commit/9be22b639ea69e102d3847dca4c53ef025e9527b, https://bugzil	O-FED-FEDO-020623/5288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			craft specific input data that can cause the program to dereference a NULL pointer when decompressing a TIFF format file, resulting in a program crash or denial of service. **CVE ID : CVE-2023-2731**	la.redhat.com/show_bug.cgi?id=2207635, https://gitlab.com/libtiff/libtiff/-/issues/548	
Vendor: gira					
Product: gira_home_server_firmware					
Affected Version(s): * Up to (including) 4.12.0.220829					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-May-2023	6.1	A vulnerability classified as problematic was found in Gira HomeServer up to 4.12.0.220829 beta. This vulnerability affects unknown code of the file /hslist. The manipulation of the argument lst with the input debug%27"><img %20src=x%20onerror=alert(document.cookie)> leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-229150 is the identifier assigned to this	N/A	O-GIR-GIRA-020623/5289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2739**		
Vendor: Google					
Product: android					
Affected Version(s): -					
Use After Free	16-May-2023	8.8	Use after free in Autofill UI in Google Chrome on Android prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) **CVE ID : CVE-2023-2722**	N/A	O-GOO-ANDR-020623/5290
Vendor: hanwhavision					
Product: ane-l6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-ANE--020623/5291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANE--020623/5292
Product: ane-l7012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANE--020623/5293
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANE--020623/5294
Product: ano-l6012r_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANO--020623/5295
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANO--020623/5296
Product: ano-l6022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANO--020623/5297
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	O-HAN-ANO--020623/5298

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: ano-l6082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANO--020623/5299
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANO--020623/5300
Product: ano-l7012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	O-HAN-ANO--020623/5301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANO--020623/5302
Product: ano-l7022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANO--020623/5303
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	O-HAN-ANO--020623/5304

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: ano-l7082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANO--020623/5305
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANO--020623/5306
Product: anv-l6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	O-HAN-ANV--020623/5307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANV--020623/5308
Product: anv-l6023r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANV--020623/5309
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-ANV--020623/5310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: anv-l6082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANV--020623/5311
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANV--020623/5312
Product: anv-l7012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-ANV--020623/5313

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANV--020623/5314
Product: anv-l7082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.03					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANV--020623/5315
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-ANV--020623/5316
Product: pnm-12082rvd_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5317
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5318
Product: pnm-7002vd_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5319
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	O-HAN-PNM--020623/5320

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: pnm-7082rvd_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5321
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5322
Product: pnm-8082vt_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	O-HAN-PNM--020623/5323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5324
Product: pnm-9000qb_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5325
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	O-HAN-PNM--020623/5326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: pnm-9000vd_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5327
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5328
Product: pnm-9002vq_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	O-HAN-PNM--020623/5329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5330
Product: pnm-9022v_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5331
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-PNM--020623/5332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: pnm-9031rv_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5333
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5334
Product: pnm-9084qz1_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-PNM--020623/5335

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5336
Product: pnm-9084rqz1_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5337
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5338
Product: pnm-9084rqz_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5339
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5340
Product: pnm-9085rqz1_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5341
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	O-HAN-PNM--020623/5342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: pnm-9085rqz_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5343
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5344
Product: pnm-9322vqp_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	O-HAN-PNM--020623/5345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5346
Product: pnm-c12083rvd_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5347
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	O-HAN-PNM--020623/5348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: pnm-c7083rvd_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5349
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5350
Product: pnm-c9022rv_firmware					
Affected Version(s): * Up to (excluding) 2.22.00					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	O-HAN-PNM--020623/5351

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-PNM--020623/5352
Product: qnd-6010r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5353
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QND--020623/5354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qnd-6011_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5355
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5356
Product: qnd-6012r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QND--020623/5357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5358
Product: qnd-6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5359
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5360
Product: qnd-6020r_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5361
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5362
Product: qnd-6021_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5363
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	O-HAN-QND--020623/5364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnd-6022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5365
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5366
Product: qnd-6030r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	O-HAN-QND--020623/5367

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5368
Product: qnd-6032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5369
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	O-HAN-QND--020623/5370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnd-6070r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5371
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5372
Product: qnd-6082r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	O-HAN-QND--020623/5373

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5374
Product: qnd-6082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5375
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QND--020623/5376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qnd-7010r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5377
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5378
Product: qnd-70142r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QND--020623/5379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5380
Product: qnd-7020r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5381
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5382
Product: qnd-7022r_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5383
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5384
Product: qnd-7030r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5385
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	O-HAN-QND--020623/5386

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnd-7032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5387
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5388
Product: qnd-7080r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	O-HAN-QND--020623/5389

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5390
Product: qnd-7082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5391
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	O-HAN-QND--020623/5392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnd-8010r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5393
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5394
Product: qnd-8011_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	O-HAN-QND--020623/5395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5396
Product: qnd-8020r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5397
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QND--020623/5398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qnd-8021_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5399
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5400
Product: qnd-8030r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QND--020623/5401

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5402
Product: qnd-8080r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5403
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QND--020623/5404
Product: qne-7080rvw_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNE--020623/5405
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNE--020623/5406
Product: qne-7088rv_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNE--020623/5407
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	O-HAN-QNE--020623/5408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qne-8011r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNE--020623/5409
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNE--020623/5410
Product: qne-8021r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	O-HAN-QNE--020623/5411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNE--020623/5412
Product: qnf-8010_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNF--020623/5413
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	O-HAN-QNF--020623/5414

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnf-9010_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNF--020623/5415
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNF--020623/5416
Product: qno-6010r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	O-HAN-QNO--020623/5417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5418
Product: qno-6012r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5419
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QNO--020623/5420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qno-6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5421
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5422
Product: qno-6020r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QNO--020623/5423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5424
Product: qno-6022r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5425
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5426
Product: qno-6022r_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5427
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5428
Product: qno-6030r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5429
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	O-HAN-QNO--020623/5430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qno-6032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5431
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5432
Product: qno-6070r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	O-HAN-QNO--020623/5433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5434
Product: qno-6082r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5435
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	O-HAN-QNO--020623/5436

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qno-6082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5437
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5438
Product: qno-7012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	O-HAN-QNO--020623/5439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5440
Product: qno-7020r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5441
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QNO--020623/5442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qno-7022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5443
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5444
Product: qno-7030r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QNO--020623/5445

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5446
Product: qno-7032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5447
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5448
Product: qno-7080r_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5449
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5450
Product: qno-7082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5451
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	O-HAN-QNO--020623/5452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qno-8010r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5453
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5454
Product: qno-8020r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	O-HAN-QNO--020623/5455

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5456
Product: qno-8030r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5457
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	O-HAN-QNO--020623/5458

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qno-8080r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5459
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNO--020623/5460
Product: qnp-6230h_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	O-HAN-QNP--020623/5461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5462
Product: qnp-6230rh_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5463
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QNP--020623/5464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qnp-6230_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5465
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5466
Product: qnp-6250h_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QNP--020623/5467

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5468
Product: qnp-6250r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5469
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5470
Product: qnp-6250_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5471
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5472
Product: qnp-6320hs_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5473
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	O-HAN-QNP--020623/5474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnp-6320h_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5475
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5476
Product: qnp-6320r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	O-HAN-QNP--020623/5477

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5478
Product: qnp-6320_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNP--020623/5479
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	O-HAN-QNP--020623/5480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnv-6010r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5481
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5482
Product: qnv-6012r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	O-HAN-QNV--020623/5483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5484
Product: qnv-6012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5485
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QNV--020623/5486

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qnv-6020r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5487
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5488
Product: qnv-6022r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QNV--020623/5489

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5490
Product: qnv-6022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5491
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5492
Product: qnv-6030r_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5493
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5494
Product: qnv-6032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5495
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	O-HAN-QNV--020623/5496

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnv-6070r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5497
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5498
Product: qnv-6082r1_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	O-HAN-QNV--020623/5499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5500
Product: qnv-6082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.14					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5501
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	O-HAN-QNV--020623/5502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnv-7010r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5503
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5504
Product: qnv-7012r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Comman	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf,	O-HAN-QNV--020623/5505

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
d Injection')			for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5506
Product: qnv-7020r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5507
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QNV--020623/5508

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				ca.com/download/50042/	
Product: qnv-7022r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5509
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5510
Product: qnv-7030r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function.	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionameri	O-HAN-QNV--020623/5511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-31996	ca.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5512
Product: qnv-7032r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5513
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5514
Product: qnv-7080r_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5515
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5516
Product: qnv-7082r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5517
Improper Neutralizat	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R	https://www.hanwhavision.	O-HAN-QNV--020623/5518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnv-8010r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5519
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5520
Product: qnv-8020r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is	https://www.hanwhavision.com/wp-	O-HAN-QNV--020623/5521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5522
Product: qnv-8030r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5523
Improper Neutralization of Input During Web Page Generation	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS).	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-	O-HAN-QNV--020623/5524

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			**CVE ID : CVE-2023-31995**	Report.pdf, https://hanwhavisionamerica.com/download/50042/	
Product: qnv-8080r_firmware					
Affected Version(s): * Up to (excluding) 1.41.05					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	8.8	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Command Injection due to improper sanitization of special characters for the NAS storage test function. **CVE ID : CVE-2023-31996**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5525
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Hanwha IP Camera ANE-L7012R 1.41.01 is vulnerable to Cross Site Scripting (XSS). **CVE ID : CVE-2023-31995**	https://www.hanwhavision.com/wp-content/uploads/2023/04/Camera-Vulnerability-Report.pdf, https://hanwhavisionamerica.com/download/50042/	O-HAN-QNV--020623/5526
Vendor: HP					
Product: hp-ux					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	19-May-2023	5.5	IBM MQ 8.0, 9.0, and 9.1 could allow a local user to obtain sensitive credential information when a detailed technical	https://www.ibm.com/support/pages/node/6985835, https://exchange.xforce.ibmcloud.com/vul	O-HP-HP-U-020623/5527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			error message is returned in a stack trace. IBM X-Force ID: 250398. **CVE ID : CVE-2023-28514**	nerabilities/250398	
N/A	19-May-2023	5.5	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose sensitive user information from a trace file if that functionality has been enabled. IBM X-Force ID: 251358. **CVE ID : CVE-2023-28950**	https://exchange.xforce.ibmcloud.com/vulnerabilities/251358, https://https://www.ibm.com/support/pages/node/6985837	O-HP-HP-U-020623/5528
Vendor: Huawei					
Product: emui					
Affected Version(s): 11.0.1					
Incorrect Permission Assignment for Critical Resource	20-May-2023	7.5	The window management module lacks permission verification.Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1692**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-EMUI-020623/5529
Improper Privilege Management	20-May-2023	7.5	The Settings module has the file privilege escalation vulnerability.Successful exploitation of this vulnerability	https://device.harmonyos.com/en/docs/security/update/security-bulletins-	O-HUA-EMUI-020623/5530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may affect confidentiality. **CVE ID : CVE-2023-1693**	202304-00000015065 28486, https://consumer.huawei.com/en/support/bulletin/2023/4/	
Improper Privilege Management	20-May-2023	7.5	The Settings module has the file privilege escalation vulnerability.Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1694**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-00000015065 28486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-EMUI-020623/5531
N/A	20-May-2023	7.5	The multimedia video module has a vulnerability in data processing.Successful exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-1696**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-00000015065 28486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-EMUI-020623/5532
Affected Version(s): 12.0					
Missing Authentication for Critical Function	26-May-2023	7.5	The reminder module lacks an authentication mechanism for broadcasts received. Successful	https://consumer.huawei.com/en/support/bulletin/2023/5/	O-HUA-EMUI-020623/5533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-0116**		
Affected Version(s): 12.0.0					
Incorrect Permission Assignment for Critical Resource	20-May-2023	7.5	The window management module lacks permission verification.Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1692**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-EMUI-020623/5534
N/A	20-May-2023	7.5	The multimedia video module has a vulnerability in data processing.Successful exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-1696**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-EMUI-020623/5535
Affected Version(s): 12.0.1					
Missing Authentication for Critical Function	26-May-2023	7.5	The reminder module lacks an authentication mechanism for broadcasts received. Successful exploitation of this	https://consumer.huawei.com/en/support/bulletin/2023/5/	O-HUA-EMUI-020623/5536

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability may affect availability. **CVE ID : CVE-2023-0116**		
Incorrect Permission Assignment for Critical Resource	20-May-2023	7.5	The window management module lacks permission verification.Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1692**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-EMUI-020623/5537
N/A	20-May-2023	7.5	The multimedia video module has a vulnerability in data processing.Successful exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-1696**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-EMUI-020623/5538
Affected Version(s): 13.0.0					
Missing Authentication for Critical Function	26-May-2023	7.5	The reminder module lacks an authentication mechanism for broadcasts received. Successful exploitation of this vulnerability may affect availability.	https://consumer.huawei.com/en/support/bulletin/2023/5/	O-HUA-EMUI-020623/5539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-0116		
Incorrect Permission Assignment for Critical Resource	20-May-2023	7.5	The window management module lacks permission verification.Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1692**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-EMUI-020623/5540
Improper Privilege Management	20-May-2023	7.5	The Settings module has the file privilege escalation vulnerability.Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1693**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-EMUI-020623/5541
Improper Privilege Management	20-May-2023	7.5	The Settings module has the file privilege escalation vulnerability.Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1694**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support	O-HUA-EMUI-020623/5542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				/bulletin/2023/4/	
N/A	20-May-2023	7.5	The multimedia video module has a vulnerability in data processing.Successful exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-1696**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-EMUI-020623/5543
Improper Authentication	26-May-2023	5.3	The online authentication provided by the hwKitAssistant lacks strict identity verification of applications. Successful exploitation of this vulnerability may affect availability of features,such as MeeTime. **CVE ID : CVE-2023-0117**	https://consumer.huawei.com/en/support/bulletin/2023/5/	O-HUA-EMUI-020623/5544
Product: harmonyos					
Affected Version(s): * Up to (excluding) 3.1.0					
Improper Privilege Management	20-May-2023	7.5	The Settings module has the file privilege escalation vulnerability.Successful exploitation of this vulnerability may affect confidentiality.	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486,	O-HUA-HARM-020623/5545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-1693	https://consumer.huawei.com/en/support/bulletin/2023/4/	
Improper Privilege Management	20-May-2023	7.5	The Settings module has the file privilege escalation vulnerability.Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1694**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-HARM-020623/5546
Affected Version(s): 2.0					
Incorrect Permission Assignment for Critical Resource	20-May-2023	7.5	The window management module lacks permission verification.Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1692**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-HARM-020623/5547
N/A	20-May-2023	7.5	The multimedia video module has a vulnerability in data processing.Successful exploitation of this vulnerability	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486,	O-HUA-HARM-020623/5548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may affect availability. **CVE ID : CVE-2023-1696**	https://consumer.huawei.com/en/support/bulletin/2023/4/	
Affected Version(s): 2.0.1					
Incorrect Permission Assignment for Critical Resource	20-May-2023	7.5	The window management module lacks permission verification.Successful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1692**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-HARM-020623/5549
N/A	20-May-2023	7.5	The multimedia video module has a vulnerability in data processing.Successful exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-1696**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-0000001506528486, https://consumer.huawei.com/en/support/bulletin/2023/4/	O-HUA-HARM-020623/5550
Affected Version(s): 2.1					
Incorrect Permission Assignment for Critical Resource	20-May-2023	7.5	The window management module lacks permission verification.Successful exploitation of this vulnerability	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202304-	O-HUA-HARM-020623/5551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may affect confidentiality. **CVE ID : CVE-2023-1692**	00000015065 28486, https://consu mer.huawei.co m/en/support /bulletin/202 3/4/	
N/A	20-May-2023	7.5	The multimedia video module has a vulnerability in data processing.Successf ul exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-1696**	https://device .harmonyos.co m/en/docs/se curity/update /security-bulletins-202304-00000015065 28486, https://consu mer.huawei.co m/en/support /bulletin/202 3/4/	O-HUA-HARM-020623/5552
Affected Version(s): 3.0.0					
Incorrect Permission Assignmen t for Critical Resource	20-May-2023	7.5	The window management module lacks permission verification.Success ful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1692**	https://device .harmonyos.co m/en/docs/se curity/update /security-bulletins-202304-00000015065 28486, https://consu mer.huawei.co m/en/support /bulletin/202 3/4/	O-HUA-HARM-020623/5553
N/A	20-May-2023	7.5	The multimedia video module has a vulnerability in data processing.Successf ul exploitation of this vulnerability	https://device .harmonyos.co m/en/docs/se curity/update /security-bulletins-202304-	O-HUA-HARM-020623/5554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			may affect availability. **CVE ID : CVE-2023-1696**	00000015065 28486, https://consu mer.huawei.co m/en/support /bulletin/202 3/4/	
Affected Version(s): 3.1.0					
Incorrect Permission Assignmen t for Critical Resource	20-May-2023	7.5	The window management module lacks permission verification.Success ful exploitation of this vulnerability may affect confidentiality. **CVE ID : CVE-2023-1692**	https://device .harmonyos.co m/en/docs/se curity/update /security-bulletins-202304-00000015065 28486, https://consu mer.huawei.co m/en/support /bulletin/202 3/4/	O-HUA-HARM-020623/5555
N/A	20-May-2023	7.5	The multimedia video module has a vulnerability in data processing.Successf ul exploitation of this vulnerability may affect availability. **CVE ID : CVE-2023-1696**	https://device .harmonyos.co m/en/docs/se curity/update /security-bulletins-202304-00000015065 28486, https://consu mer.huawei.co m/en/support /bulletin/202 3/4/	O-HUA-HARM-020623/5556
Vendor: IBM					
Product: aix					
Affected Version(s): -					
Deserializa tion of	22-May-2023	9.8	IBM InfoSphere Information Server 11.7 is affected by a	https://www.i bm.com/supp ort/pages/no	O-IBM-AIX-020623/5557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			remote code execution vulnerability due to insecure deserialization in an RMI service. IBM X-Force ID: 255285. **CVE ID : CVE-2023-32336**	de/6995879, https://exchange.xforce.ibmcloud.com/vulnerabilities/255285	
Cleartext Storage of Sensitive Information	19-May-2023	5.5	IBM InfoSphere Information Server 11.7 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 244373. **CVE ID : CVE-2023-22878**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244373, https://https://www.ibm.com/support/pages/node/6988155	O-IBM-AIX-020623/5558
Generation of Error Message Containing Sensitive Information	19-May-2023	5.5	IBM MQ 8.0, 9.0, and 9.1 could allow a local user to obtain sensitive credential information when a detailed technical error message is returned in a stack trace. IBM X-Force ID: 250398. **CVE ID : CVE-2023-28514**	https://www.ibm.com/support/pages/node/6985835, https://exchange.xforce.ibmcloud.com/vulnerabilities/250398	O-IBM-AIX-020623/5559
N/A	19-May-2023	5.5	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose sensitive user information from a trace file if that functionality has been enabled. IBM	https://exchange.xforce.ibmcloud.com/vulnerabilities/251358, https://https://www.ibm.com/support/	O-IBM-AIX-020623/5560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			X-Force ID: 251358. **CVE ID : CVE-2023-28950**	pages/node/6985837	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 251213. **CVE ID : CVE-2023-28529**	https://www.ibm.com/support/pages/node/6988675, https://https://exchange.xforce.ibmcloud.com/vulnerabilities/251213	O-IBM-AIX-020623/5561
Product: i					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	19-May-2023	5.5	IBM MQ 8.0, 9.0, and 9.1 could allow a local user to obtain sensitive credential information when a detailed technical error message is returned in a stack trace. IBM X-Force ID: 250398. **CVE ID : CVE-2023-28514**	https://www.ibm.com/support/pages/node/6985835, https://exchange.xforce.ibmcloud.com/vulnerabilities/250398	O-IBM-I-020623/5562
N/A	19-May-2023	5.5	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3	https://exchange.xforce.ibm	O-IBM-I-020623/5563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could disclose sensitive user information from a trace file if that functionality has been enabled. IBM X-Force ID: 251358. **CVE ID : CVE-2023-28950**	cloud.com/vulnerabilities/251358, https://https://www.ibm.com/support/pages/node/6985837	
Product: powervm_hypervisor					
Affected Version(s): From (including) fw1010 Up to (including) fw1010.50					
Improper Input Validation	23-May-2023	7.9	IBM PowerVM Hypervisor FW860.00 through FW860.B3, FW950.00 through FW950.70, FW1010.00 through FW1010.50, FW1020.00 through FW1020.30, and FW1030.00 through FW1030.10 could allow a local attacker with control a partition that has been assigned SRIOV virtual function (VF) to cause a denial of service to a peer partition or arbitrary data corruption. IBM X-Force ID: 253175. **CVE ID : CVE-2023-30440**	https://www.ibm.com/support/pages/node/6997133, https://exchange.xforce.ibmcloud.com/vulnerabilities/253175	O-IBM-POWE-020623/5564
Affected Version(s): From (including) fw1010.00 Up to (excluding) fw1010.51					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	O-IBM-POWE-020623/5565
Affected Version(s): From (including) fw1020.00 Up to (excluding) fw1020.31					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	O-IBM-POWE-020623/5566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**		
Affected Version(s): From (including) fw1020.00 Up to (including) fw1020.30					
Improper Input Validation	23-May-2023	7.9	IBM PowerVM Hypervisor FW860.00 through FW860.B3, FW950.00 through FW950.70, FW1010.00 through FW1010.50, FW1020.00 through FW1020.30, and FW1030.00 through FW1030.10 could allow a local attacker with control a partition that has been assigned SRIOV virtual function (VF) to cause a denial of service to a peer partition or arbitrary data corruption. IBM X-Force ID: 253175. **CVE ID : CVE-2023-30440**	https://www.ibm.com/support/pages/node/6997133, https://exchange.xforce.ibmcloud.com/vulnerabilities/253175	O-IBM-POWE-020623/5567

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) fw1030.00 Up to (excluding) fw1030.11					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	O-IBM-POWE-020623/5568
Affected Version(s): From (including) fw1030.00 Up to (including) fw1030.10					
Improper Input Validation	23-May-2023	7.9	IBM PowerVM Hypervisor FW860.00 through FW860.B3, FW950.00 through FW950.70, FW1010.00 through FW1010.50, FW1020.00 through FW1020.30, and FW1030.00 through	https://www.ibm.com/support/pages/node/6997133, https://exchange.xforce.ibmcloud.com/vulnerabilities/253175	O-IBM-POWE-020623/5569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW1030.10 could allow a local attacker with control a partition that has been assigned SRIOV virtual function (VF) to cause a denial of service to a peer partition or arbitrary data corruption. IBM X-Force ID: 253175. **CVE ID : CVE-2023-30440**		
Affected Version(s): From (including) fw860 Up to (including) fw860.b3					
Improper Input Validation	23-May-2023	7.9	IBM PowerVM Hypervisor FW860.00 through FW860.B3, FW950.00 through FW950.70, FW1010.00 through FW1010.50, FW1020.00 through FW1020.30, and FW1030.00 through FW1030.10 could allow a local attacker with control a partition that has been assigned SRIOV virtual function (VF) to cause a denial of service to a peer partition or arbitrary data corruption. IBM X-Force ID: 253175.	https://www.ibm.com/support/pages/node/6997133, https://exchange.xforce.ibmcloud.com/vulnerabilities/253175	O-IBM-POWE-020623/5570

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-30440		
Affected Version(s): From (including) fw950 Up to (excluding) fw950.71					
N/A	17-May-2023	8.8	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706. **CVE ID : CVE-2023-30438**	https://www.ibm.com/support/pages/node/6993021, https://exchange.xforce.ibmcloud.com/vulnerabilities/252706	O-IBM-POWE-020623/5571
Affected Version(s): From (including) fw950 Up to (including) fw950.70					
Improper Input Validation	23-May-2023	7.9	IBM PowerVM Hypervisor FW860.00 through FW860.B3, FW950.00 through FW950.70, FW1010.00 through FW1010.50, FW1020.00 through	https://www.ibm.com/support/pages/node/6997133, https://exchange.xforce.ibmcloud.com/vulnerabilities/253175	O-IBM-POWE-020623/5572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			FW1020.30, and FW1030.00 through FW1030.10 could allow a local attacker with control a partition that has been assigned SRIOV virtual function (VF) to cause a denial of service to a peer partition or arbitrary data corruption. IBM X-Force ID: 253175. **CVE ID : CVE-2023-30440**		
Vendor: icom					
Product: sr-7100vn\#31_firmware					
Affected Version(s): * Up to (excluding) 1.22					
N/A	23-May-2023	6.8	Privilege escalation vulnerability in SR-7100VN firmware Ver.1.38(N) and earlier and SR-7100VN #31 firmware Ver.1.21 and earlier allows a network-adjacent attacker with administrative privilege of the affected product to obtain an administrative privilege of the OS (Operating System). As a result, an arbitrary OS command may be executed.	https://www.icom.co.jp/news/7239/	O-ICO-SR-7-020623/5573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28390		
Product: sr-7100vn_firmware					
Affected Version(s): * Up to (excluding) 1.39\\(n\\)					
N/A	23-May-2023	6.8	Privilege escalation vulnerability in SR-7100VN firmware Ver.1.38(N) and earlier and SR-7100VN #31 firmware Ver.1.21 and earlier allows a network-adjacent attacker with administrative privilege of the affected product to obtain an administrative privilege of the OS (Operating System). As a result, an arbitrary OS command may be executed. **CVE ID : CVE-2023-28390**	https://www.icom.co.jp/news/7239/	O-ICO-SR-7-020623/5574
Vendor: inaba					
Product: ac-wapu-300-p_firmware					
Affected Version(s): * Up to (including) 1.00_b08p					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	7.2	Wi-Fi AP UNIT AC-WAPU-300 v1.00_B07 and earlier, AC-WAPU-300-P v1.00_B08P and earlier, AC-WAPUM-300 v1.00_B07 and earlier, and AC-WAPUM-300-P v1.00_B08P and	N/A	O-INA-AC-W-020623/5575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-28392**		
Product: ac-wapu-300_firmware					
Affected Version(s): * Up to (including) 1.00_b07					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	7.2	Wi-Fi AP UNIT AC-WAPU-300 v1.00_B07 and earlier, AC-WAPU-300-P v1.00_B08P and earlier, AC-WAPUM-300 v1.00_B07 and earlier, and AC-WAPUM-300-P v1.00_B08P and earlier allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-28392**	N/A	O-INA-AC-W-020623/5576
Product: ac-wapum-300-p_firmware					
Affected Version(s): * Up to (including) 1.00_b08p					
Improper Neutralization of Special Elements used in an	23-May-2023	7.2	Wi-Fi AP UNIT AC-WAPU-300 v1.00_B07 and earlier, AC-WAPU-300-P v1.00_B08P and earlier, AC-	N/A	O-INA-AC-W-020623/5577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			WAPUM-300 v1.00_B07 and earlier, and AC-WAPUM-300-P v1.00_B08P and earlier allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-28392**		
Product: ac-wapum-300_firmware					
Affected Version(s): * Up to (including) 1.00_b07					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-May-2023	7.2	Wi-Fi AP UNIT AC-WAPU-300 v1.00_B07 and earlier, AC-WAPU-300-P v1.00_B08P and earlier, AC-WAPUM-300 v1.00_B07 and earlier, and AC-WAPUM-300-P v1.00_B08P and earlier allow a remote authenticated attacker with an administrative privilege to execute an arbitrary OS command. **CVE ID : CVE-2023-28392**	N/A	O-INA-AC-W-020623/5578
Vendor: jins					
Product: jins_meme_firmware					
Affected Version(s): * Up to (excluding) 2.3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	23-May-2023	6.5	JINS MEME CORE Firmware version 2.2.0 and earlier uses a hard-coded cryptographic key, which may lead to data acquired by a sensor of the affected product being decrypted by a network-adjacent attacker. **CVE ID : CVE-2023-27921**	N/A	O-JIN-JINS-020623/5579
Vendor: Johnsoncontrols					
Product: openblue_enterprise_manager_data_collector					
Affected Version(s): * Up to (excluding) 3.2.5.75					
Improper Authentication	18-May-2023	7.5	Improper authentication in OpenBlue Enterprise Manager Data Collector versions prior to 3.2.5.75 allow access to an unauthorized user under certain circumstances. **CVE ID : CVE-2023-2024**	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	O-JOH-OPEN-020623/5580
Exposure of Resource to Wrong Sphere	18-May-2023	6.5	OpenBlue Enterprise Manager Data Collector versions prior to 3.2.5.75 may expose sensitive information to an unauthorized user under certain circumstances.	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	O-JOH-OPEN-020623/5581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-2025		
Vendor: kaiostech					
Product: kaios					
Affected Version(s): 3.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-May-2023	9.8	An issue was discovered in KaiOS 3.0 before 3.1. The /system/bin/tctweb_server binary exposes a local web server that responds to GET and POST requests on port 2929. The server accepts arbitrary Bash commands and executes them as root. Because it is not permission or context restricted and returns proper CORS headers, it's accessible to all websites via the browser. At a bare minimum, this allows an attacker to retrieve a list of the user's installed apps, notifications, and downloads. It also allows an attacker to delete local files and modify system properties including the boolean persist.moz.killswitch property (which would render the	https://kaios.dev/cve/1411380	O-KAI-KAIO-020623/5582

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			device inoperable). This vulnerability is partially mitigated by SELinux which prevents reads, writes, or modifications to files or permissions within protected partitions. **CVE ID : CVE-2023-33294**		
Exposure of Resource to Wrong Sphere	22-May-2023	5.3	An issue was discovered in KaiOS 3.0 and 3.1. The binary /system/kaios/api-daemon exposes a local web server on *.localhost with subdomains for each installed applications, e.g., myapp.localhost. An attacker can make fetch requests to api-deamon to determine if a given app is installed and read the manifest.webmanifest contents, including the app version. **CVE ID : CVE-2023-33293**	https://kaios.dev/cve/1410290	O-KAI-KAIO-020623/5583
Affected Version(s): 3.1					
Improper Neutralization of Special	22-May-2023	9.8	An issue was discovered in KaiOS 3.0 before 3.1. The /system/bin/tctwe	https://kaios.dev/cve/1411380	O-KAI-KAIO-020623/5584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			b_server binary exposes a local web server that responds to GET and POST requests on port 2929. The server accepts arbitrary Bash commands and executes them as root. Because it is not permission or context restricted and returns proper CORS headers, it's accessible to all websites via the browser. At a bare minimum, this allows an attacker to retrieve a list of the user's installed apps, notifications, and downloads. It also allows an attacker to delete local files and modify system properties including the boolean persist.moz.killswitch property (which would render the device inoperable). This vulnerability is partially mitigated by SELinux which prevents reads, writes, or modifications to files or permissions within protected partitions.		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33294		
Exposure of Resource to Wrong Sphere	22-May-2023	5.3	An issue was discovered in KaiOS 3.0 and 3.1. The binary /system/kaios/api-daemon exposes a local web server on *.localhost with subdomains for each installed applications, e.g., myapp.localhost. An attacker can make fetch requests to api-deamon to determine if a given app is installed and read the manifest.webmanifest contents, including the app version. **CVE ID : CVE-2023-33293**	https://kaios.dev/cve/1410290	O-KAI-KAIO-020623/5585
Vendor: Linksys					
Product: e2000_firmware					
Affected Version(s): 1.0.06					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	7.2	There is a command injection vulnerability in the Linksys E2000 router with firmware version 1.0.06. If an attacker gains web management privileges, they can inject commands into the post	N/A	O-LIN-E200-020623/5586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request parameters WL_atten_bb, WL_atten_radio, and WL_atten_ctl in the apply.cgi interface, thereby gaining shell privileges. **CVE ID : CVE-2023-31740**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-May-2023	7.2	There is a command injection vulnerability in the Linksys E2000 router with firmware version 1.0.06. If an attacker gains web management privileges, they can inject commands into the post request parameters wl_ssid, wl_ant, wl_rate, WL_atten_ctl, ttcp_num, ttcp_size in the httpd s Start_EPI() function, thereby gaining shell privileges. **CVE ID : CVE-2023-31741**	N/A	O-LIN-E200-020623/5587
Product: wrt54gl_firmware					
Affected Version(s): 4.30.18.006					
Improper Neutralization of Special Elements used in a	22-May-2023	7.2	There is a command injection vulnerability in the Linksys WRT54GL router with firmware version	N/A	O-LIN-WRT5-020623/5588

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			4.30.18.006. If an attacker gains web management privileges, they can inject commands into the post request parameters wl_ant, wl_rate, WL_atten_ctl, ttcp_num, ttcp_size in the httpd s Start_EPI() function, thereby gaining shell privileges. **CVE ID : CVE-2023-31742**		
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Deserialization of Untrusted Data	22-May-2023	9.8	IBM InfoSphere Information Server 11.7 is affected by a remote code execution vulnerability due to insecure deserialization in an RMI service. IBM X-Force ID: 255285. **CVE ID : CVE-2023-32336**	https://www.ibm.com/support/pages/node/6995879, https://exchange.xforce.ibmcloud.com/vulnerabilities/255285	O-LIN-LINU-020623/5589
Improper Neutralization of Input During Web Page Generation	23-May-2023	6.1	Cross-site Scripting vulnerability in Hitachi Ops Center Analyzer (Hitachi Ops Center Analyzer detail view component) allows Reflected XSS.This issue	https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2023-	O-LIN-LINU-020623/5590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			affects Hitachi Ops Center Analyzer: from 10.9.1-00 before 10.9.2-00. **CVE ID : CVE-2023-30469**	115/index.html	
Cleartext Storage of Sensitive Information	19-May-2023	5.5	IBM InfoSphere Information Server 11.7 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 244373. **CVE ID : CVE-2023-22878**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244373, https://https://www.ibm.com/support/pages/node/6988155	O-LIN-LINU-020623/5591
Generation of Error Message Containing Sensitive Information	19-May-2023	5.5	IBM MQ 8.0, 9.0, and 9.1 could allow a local user to obtain sensitive credential information when a detailed technical error message is returned in a stack trace. IBM X-Force ID: 250398. **CVE ID : CVE-2023-28514**	https://www.ibm.com/support/pages/node/6985835, https://exchange.xforce.ibmcloud.com/vulnerabilities/250398	O-LIN-LINU-020623/5592
N/A	19-May-2023	5.5	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose sensitive user information from a trace file if that functionality has been enabled. IBM X-Force ID: 251358.	https://exchange.xforce.ibmcloud.com/vulnerabilities/251358, https://https://www.ibm.com/support/pages/node/6985837	O-LIN-LINU-020623/5593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-28950		
N/A	21-May-2023	5.5	When Akka HTTP before 10.5.2 accepts file uploads via the FileUploadDirectives.fileUploadAll directive, the temporary file it creates has too weak permissions: it is readable by other users on Linux or UNIX, a similar issue to CVE-2022-41946. **CVE ID : CVE-2023-33251**	https://akka.io/security/akka-http-cve-2023-05-15.html	O-LIN-LINU-020623/5594
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 251213. **CVE ID : CVE-2023-28529**	https://www.ibm.com/support/pages/node/6988675, https://https://exchange.xforce.ibmcloud.com/vulnerabilities/251213	O-LIN-LINU-020623/5595
Affected Version(s): * Up to (excluding) 6.1					
Use After Free	18-May-2023	5.5	A use-after-free flaw was found in	https://github.com/torvalds	O-LIN-LINU-020623/5596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			reconn_set_ipaddr_from_hostname in fs/cifs/connect.c in the Linux kernel. The issue occurs when it forgets to set the free pointer server->hostname to NULL, leading to an invalid pointer request. **CVE ID : CVE-2023-1195**	/linux/commit/153695d36ead0ccc4d0256953c751cabf673e621	
Affected Version(s): * Up to (excluding) 6.2.9					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-May-2023	6.4	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/net/ethernet/qualcomm/emac/emac.c if a physically proximate attacker unplugs an emac based device. **CVE ID : CVE-2023-33203**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6b6bc5b8bd2d4ca9e1efa9ae0f98a0b0687ace75	O-LIN-LINU-020623/5597
Use After Free	22-May-2023	4.7	An issue was discovered in the Linux kernel before 6.2.9. A use-after-free was found in bq24190_remove in drivers/power/supply/bq24190_charger.c. It could allow a local attacker to crash the system due to a race condition.	https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=47c29d69212911f50bdcdd0564b5999a559010d4, https://lore.kernel.org/all/CAHk-=whcaHLNpb7Mu_QX7ABw	O-LIN-LINU-020623/5598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33288	PgyRyfW-V8=v4Mv0S22fpjY4JQ@mail.gmail.com/	
Affected Version(s): * Up to (including) 6.2					
Use After Free	17-May-2023	4.7	A use-after-free flaw was found in xen_9pfs_front_removet in net/9p/trans_xen.c in Xen transport for 9pfs in the Linux Kernel. This flaw could allow a local attacker to crash the system due to a race problem, possibly leading to a kernel information leak. **CVE ID : CVE-2023-1859**	https://lore.kernel.org/all/20230313090002.3308025-1-zyytlz.wz@163.com/	O-LIN-LINU-020623/5599
Affected Version(s): 6.1					
Use After Free	18-May-2023	5.5	A use-after-free flaw was found in reconn_set_ipaddr_from_hostname in fs/cifs/connect.c in the Linux kernel. The issue occurs when it forgets to set the free pointer server->hostname to NULL, leading to an invalid pointer request. **CVE ID : CVE-2023-1195**	https://github.com/torvalds/linux/commit/153695d36ead0ccc4d0256953c751cabf673e621	O-LIN-LINU-020623/5600
Affected Version(s): 6.3					
Use After Free	21-May-2023	9.8	The Linux kernel 6.3 has a use-after-	https://lore.kernel.org/linu	O-LIN-LINU-020623/5601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			free in iopt_unmap_iova_range in drivers/iommu/iommufd/io_pagetable.c. **CVE ID : CVE-2023-33250**	x-iommu/ZDabT%2FuRl%2FjxFhm0@ip-172-31-85-199.ec2.internal/T/	
Use After Free	17-May-2023	4.7	A use-after-free flaw was found in xen_9pfs_front_removet in net/9p/trans_xen.c in Xen transport for 9pfs in the Linux Kernel. This flaw could allow a local attacker to crash the system due to a race problem, possibly leading to a kernel information leak. **CVE ID : CVE-2023-1859**	https://lore.kernel.org/all/20230313090002.3308025-1-zyytlz.wz@163.com/	O-LIN-LINU-020623/5602
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					
Deserialization of Untrusted Data	22-May-2023	9.8	IBM InfoSphere Information Server 11.7 is affected by a remote code execution vulnerability due to insecure deserialization in an RMI service. IBM X-Force ID: 255285. **CVE ID : CVE-2023-32336**	https://www.ibm.com/support/pages/node/6995879, https://exchange.xforce.ibmcloud.com/vulnerabilities/255285	O-MIC-WIND-020623/5603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	24-May-2023	7.8	A vulnerability classified as critical was found in Twister Antivirus 8. This vulnerability affects the function 0x804f2143/0x804f217f/0x804f214b/0x80800043 in the library filppd.sys of the component IoControlCode Handler. The manipulation leads to memory corruption. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-229852. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2873**	N/A	O-MIC-WIND-020623/5604
N/A	19-May-2023	7.8	Foxit PDF Reader (12.1.1.15289 and earlier) and Foxit PDF Editor (12.1.1.15289 and all previous 12.x versions, 11.2.5.53785 and all previous 11.x versions, and	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-020623/5605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			10.1.11.37866 and earlier) on Windows allows Local Privilege Escalation when installed to a non-default directory because unprivileged users have access to an executable file of a system service. This is fixed in 12.1.2. **CVE ID : CVE-2023-33240**		
Cleartext Storage of Sensitive Information	19-May-2023	5.5	IBM InfoSphere Information Server 11.7 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 244373. **CVE ID : CVE-2023-22878**	https://exchange.xforce.ibmcloud.com/vulnerabilities/244373, https://https://www.ibm.com/support/pages/node/6988155	O-MIC-WIND-020623/5606
Generation of Error Message Containing Sensitive Information	19-May-2023	5.5	IBM MQ 8.0, 9.0, and 9.1 could allow a local user to obtain sensitive credential information when a detailed technical error message is returned in a stack trace. IBM X-Force ID: 250398. **CVE ID : CVE-2023-28514**	https://www.ibm.com/support/pages/node/6985835, https://exchange.xforce.ibmcloud.com/vulnerabilities/250398	O-MIC-WIND-020623/5607
N/A	24-May-2023	5.5	A vulnerability, which was classified as	N/A	O-MIC-WIND-020623/5608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			problematic, has been found in Twister Antivirus 8. This issue affects the function 0x804f2158/0x804f2154/0x804f2150/0x804f215c/0x804f2160/0x80800040/0x804f214c/0x804f2148/0x804f2144/0x801120e4/0x804f213c/0x804f2140 in the library filppd.sys of the component IoControlCode Handler. The manipulation leads to denial of service. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. The identifier VDB-229853 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2874**		
N/A	19-May-2023	5.5	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose sensitive user information from a trace file if that	https://exchange.xforce.ibmcloud.com/vulnerabilities/251358, https://https:	O-MIC-WIND-020623/5609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functionality has been enabled. IBM X-Force ID: 251358. **CVE ID : CVE-2023-28950**	//www.ibm.com/support/pages/node/6985837	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-May-2023	5.4	IBM InfoSphere Information Server 11.7 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 251213. **CVE ID : CVE-2023-28529**	https://www.ibm.com/support/pages/node/6988675, https://https://exchange.xforce.ibmcloud.com/vulnerabilities/251213	O-MIC-WIND-020623/5610
N/A	17-May-2023	4.3	Data leakage in Adobe connector in Snow Software SPE 9.27.0 on Windows allows privileged user to observe other users data. **CVE ID : CVE-2023-2679**	https://community.snowsoftware.com/s/feed/0D56M00009Ex9dySAB	O-MIC-WIND-020623/5611
Vendor: Mitsubishielectric					
Product: melsec_ws0-geth00200_firmware					
Affected Version(s): *					
Insecure Default Initializatio	19-May-2023	8.6	Active Debug Code vulnerability in Mitsubishi Electric	https://www.mitsubishielectric.com/en/p	O-MIT-MELS-020623/5612

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n of Resource			Corporation MELSEC WS Series WS0-GETH00200 all versions allows a remote unauthenticated attacker to bypass authentication and illegally log into the affected module by connecting to it via telnet which is hidden function and is enabled by default when shipped from the factory. As a result, a remote attacker with unauthorized login can reset the module, and if certain conditions are met, he/she can disclose or tamper with the module's configuration or rewrite the firmware. **CVE ID : CVE-2023-1618**	sirt/vulnerability/pdf/2023-002_en.pdf	
Vendor: nissan					
Product: sylphy_classic_2021_firmware					
Affected Version(s): -					
Authentication Bypass by Capture-replay	22-May-2023	6.5	The remote keyfob system on Nissan Sylphy Classic 2021 sends the same RF signal for each door-open request, which allows for a replay attack.	N/A	O-NIS-SYLP-020623/5613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-33281		
Vendor: Oracle					
Product: solaris					
Affected Version(s): -					
Generation of Error Message Containing Sensitive Information	19-May-2023	5.5	IBM MQ 8.0, 9.0, and 9.1 could allow a local user to obtain sensitive credential information when a detailed technical error message is returned in a stack trace. IBM X-Force ID: 250398. **CVE ID : CVE-2023-28514**	https://www.ibm.com/support/pages/node/6985835, https://exchange.xforce.ibmcloud.com/vulnerabilities/250398	O-ORA-SOLA-020623/5614
N/A	19-May-2023	5.5	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose sensitive user information from a trace file if that functionality has been enabled. IBM X-Force ID: 251358. **CVE ID : CVE-2023-28950**	https://exchange.xforce.ibmcloud.com/vulnerabilities/251358, https://https://www.ibm.com/support/pages/node/6985837	O-ORA-SOLA-020623/5615
Vendor: qrio					
Product: q-sl2_firmware					
Affected Version(s): * Up to (including) 2.0.9					
Improper Authentication	23-May-2023	8.8	Authentication bypass vulnerability in Qrio Lock (Q-SL2) firmware version 2.0.9 and earlier allows a network-	https://qrio.me/article/announce/2023/4140/	O-QRI-Q-SL-020623/5616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker to analyze the product's communication data and conduct an arbitrary operation under certain conditions. **CVE ID : CVE-2023-25946**		
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
Use After Free	17-May-2023	8.8	A flaw was found in the WebKitGTK package. An improper input validation issue may lead to a use-after-free vulnerability. This flaw allows attackers with network access to pass specially crafted web content files, causing a denial of service or arbitrary code execution. This CVE exists because of a CVE-2023-28205 security regression for the WebKitGTK package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2203**	N/A	O-RED-ENTE-020623/5617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	7.8	A flaw was found in the Emacs text editor. Processing a specially crafted org-mode code with the "org-babel-execute:latex" function in ob-latex.el can result in arbitrary command execution. This CVE exists because of a CVE-2023-28617 security regression for the emacs package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2491**	N/A	O-RED-ENTE-020623/5618
N/A	17-May-2023	7.5	A vulnerability was found in the libreswan library. This security issue occurs when an IKEv1 Aggressive Mode packet is received with only unacceptable crypto algorithms, and the response packet is not sent with a zero responder SPI. When a subsequent packet is received where the sender reuses the libreswan responder SPI as its	N/A	O-RED-ENTE-020623/5619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			own initiator SPI, the pluto daemon state machine crashes. No remote code execution is possible. This CVE exists because of a CVE-2023-30570 security regression for libreswan package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2295**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-May-2023	6.4	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/net/ethernet/qualcomm/emac/emac.c if a physically proximate attacker unplugs an emac based device. **CVE ID : CVE-2023-33203**	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6b6bc5b8bd2d4ca9e1efa9ae0f98a0b0687ace75	O-RED-ENTE-020623/5620
Affected Version(s): 9.0					
Use After Free	17-May-2023	8.8	A flaw was found in the WebKitGTK package. An improper input validation issue may lead to a use-after-free vulnerability. This flaw allows attackers with	N/A	O-RED-ENTE-020623/5621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			network access to pass specially crafted web content files, causing a denial of service or arbitrary code execution. This CVE exists because of a CVE-2023-28205 security regression for the WebKitGTK package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2203**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	7.8	A flaw was found in the Emacs text editor. Processing a specially crafted org-mode code with the "org-babel-execute:latex" function in ob-latex.el can result in arbitrary command execution. This CVE exists because of a CVE-2023-28617 security regression for the emacs package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2491**	N/A	O-RED-ENTE-020623/5622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-May-2023	7.5	A vulnerability was found in the libreswan library. This security issue occurs when an IKEv1 Aggressive Mode packet is received with only unacceptable crypto algorithms, and the response packet is not sent with a zero responder SPI. When a subsequent packet is received where the sender reuses the libreswan responder SPI as its own initiator SPI, the pluto daemon state machine crashes. No remote code execution is possible. This CVE exists because of a CVE-2023-30570 security regression for libreswan package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2295**	N/A	O-RED-ENTE-020623/5623
Concurrent Execution using Shared Resource with	18-May-2023	6.4	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/net/ethern	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6b	O-RED-ENTE-020623/5624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			et/qualcomm/emac/emac.c if a physically proximate attacker unplugs an emac based device. **CVE ID : CVE-2023-33203**	6bc5b8bd2d4ca9e1efa9ae0f98a0b0687ace75	
NULL Pointer Dereference	17-May-2023	5.5	A NULL pointer dereference flaw was found in Libtiff's LZWDecode() function in the libtiff/tif_lzw.c file. This flaw allows a local attacker to craft specific input data that can cause the program to dereference a NULL pointer when decompressing a TIFF format file, resulting in a program crash or denial of service. **CVE ID : CVE-2023-2731**	https://github.com/libsdl-org/libtiff/commit/9be22b639ea69e102d3847dca4c53ef025e9527b, https://bugzilla.redhat.com/show_bug.cgi?id=2207635, https://gitlab.com/libtiff/libtiff/-/issues/548	O-RED-ENTE-020623/5625
Product: enterprise_linux_eus					
Affected Version(s): 8.8					
Use After Free	17-May-2023	8.8	A flaw was found in the WebKitGTK package. An improper input validation issue may lead to a use-after-free vulnerability. This flaw allows attackers with network access to	N/A	O-RED-ENTE-020623/5626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			pass specially crafted web content files, causing a denial of service or arbitrary code execution. This CVE exists because of a CVE-2023-28205 security regression for the WebKitGTK package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2203**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	7.8	A flaw was found in the Emacs text editor. Processing a specially crafted org-mode code with the "org-babel-execute:latex" function in ob-latex.el can result in arbitrary command execution. This CVE exists because of a CVE-2023-28617 security regression for the emacs package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2491**	N/A	O-RED-ENTE-020623/5627
N/A	17-May-2023	7.5	A vulnerability was found in the libreswan library.	N/A	O-RED-ENTE-020623/5628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This security issue occurs when an IKEv1 Aggressive Mode packet is received with only unacceptable crypto algorithms, and the response packet is not sent with a zero responder SPI. When a subsequent packet is received where the sender reuses the libreswan responder SPI as its own initiator SPI, the pluto daemon state machine crashes. No remote code execution is possible. This CVE exists because of a CVE-2023-30570 security regression for libreswan package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2295**		
Affected Version(s): 9.2					
Use After Free	17-May-2023	8.8	A flaw was found in the WebKitGTK package. An improper input validation issue may lead to a use-after-free vulnerability. This	N/A	O-RED-ENTE-020623/5629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			flaw allows attackers with network access to pass specially crafted web content files, causing a denial of service or arbitrary code execution. This CVE exists because of a CVE-2023-28205 security regression for the WebKitGTK package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2203**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	7.8	A flaw was found in the Emacs text editor. Processing a specially crafted org-mode code with the "org-babel-execute:latex" function in ob-latex.el can result in arbitrary command execution. This CVE exists because of a CVE-2023-28617 security regression for the emacs package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2491**	N/A	O-RED-ENTE-020623/5630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	17-May-2023	7.5	A vulnerability was found in the libreswan library. This security issue occurs when an IKEv1 Aggressive Mode packet is received with only unacceptable crypto algorithms, and the response packet is not sent with a zero responder SPI. When a subsequent packet is received where the sender reuses the libreswan responder SPI as its own initiator SPI, the pluto daemon state machine crashes. No remote code execution is possible. This CVE exists because of a CVE-2023-30570 security regression for libreswan package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2295**	N/A	O-RED-ENTE-020623/5631
Product: enterprise_linux_high_availability					
Affected Version(s): 9.0					
N/A	17-May-2023	9.8	It was discovered that an update for PCS package in RHBA-2023:2151	N/A	O-RED-ENTE-020623/5632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			erratum released as part of Red Hat Enterprise Linux 9.2 failed to include the fix for the Webpack issue CVE-2023-28154 (for PCS package), which was previously addressed in Red Hat Enterprise Linux 9.1 via erratum RHSA-2023:1591. The CVE-2023-2319 was assigned to that Red Hat specific security regression in Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2319**		
Product: enterprise_linux_high_availability_eus					
Affected Version(s): 9.2					
N/A	17-May-2023	9.8	It was discovered that an update for PCS package in RHBA-2023:2151 erratum released as part of Red Hat Enterprise Linux 9.2 failed to include the fix for the Webpack issue CVE-2023-28154 (for PCS package), which was previously addressed in Red Hat Enterprise Linux 9.1 via	N/A	O-RED-ENTE-020623/5633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			erratum RHSA-2023:1591. The CVE-2023-2319 was assigned to that Red Hat specific security regression in Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2319**		
Product: enterprise_linux_server_aus					
Affected Version(s): 8.8					
Use After Free	17-May-2023	8.8	A flaw was found in the WebKitGTK package. An improper input validation issue may lead to a use-after-free vulnerability. This flaw allows attackers with network access to pass specially crafted web content files, causing a denial of service or arbitrary code execution. This CVE exists because of a CVE-2023-28205 security regression for the WebKitGTK package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2203**	N/A	O-RED-ENTE-020623/5634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	7.8	A flaw was found in the Emacs text editor. Processing a specially crafted org-mode code with the "org-babel-execute:latex" function in ob-latex.el can result in arbitrary command execution. This CVE exists because of a CVE-2023-28617 security regression for the emacs package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2491**	N/A	O-RED-ENTE-020623/5635
N/A	17-May-2023	7.5	A vulnerability was found in the libreswan library. This security issue occurs when an IKEv1 Aggressive Mode packet is received with only unacceptable crypto algorithms, and the response packet is not sent with a zero responder SPI. When a subsequent packet is received where the sender reuses the libreswan responder SPI as its	N/A	O-RED-ENTE-020623/5636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			own initiator SPI, the pluto daemon state machine crashes. No remote code execution is possible. This CVE exists because of a CVE-2023-30570 security regression for libreswan package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2295**		
Affected Version(s): 9.2					
Use After Free	17-May-2023	8.8	A flaw was found in the WebKitGTK package. An improper input validation issue may lead to a use-after-free vulnerability. This flaw allows attackers with network access to pass specially crafted web content files, causing a denial of service or arbitrary code execution. This CVE exists because of a CVE-2023-28205 security regression for the WebKitGTK package in Red Hat Enterprise Linux 8.8 and Red Hat	N/A	O-RED-ENTE-020623/5637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Linux 9.2. **CVE ID : CVE-2023-2203**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	7.8	A flaw was found in the Emacs text editor. Processing a specially crafted org-mode code with the "org-babel-execute:latex" function in ob-latex.el can result in arbitrary command execution. This CVE exists because of a CVE-2023-28617 security regression for the emacs package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2491**	N/A	O-RED-ENTE-020623/5638
N/A	17-May-2023	7.5	A vulnerability was found in the libreswan library. This security issue occurs when an IKEv1 Aggressive Mode packet is received with only unacceptable crypto algorithms, and the response packet is not sent with a zero responder SPI. When a subsequent packet is received	N/A	O-RED-ENTE-020623/5639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			where the sender reuses the libreswan responder SPI as its own initiator SPI, the pluto daemon state machine crashes. No remote code execution is possible. This CVE exists because of a CVE-2023-30570 security regression for libreswan package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2295**		
Product: enterprise_linux_server_tus					
Affected Version(s): 8.8					
Use After Free	17-May-2023	8.8	A flaw was found in the WebKitGTK package. An improper input validation issue may lead to a use-after-free vulnerability. This flaw allows attackers with network access to pass specially crafted web content files, causing a denial of service or arbitrary code execution. This CVE exists because of a CVE-2023-28205 security regression	N/A	O-RED-ENTE-020623/5640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			for the WebKitGTK package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2203**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	7.8	A flaw was found in the Emacs text editor. Processing a specially crafted org-mode code with the "org-babel-execute:latex" function in ob-latex.el can result in arbitrary command execution. This CVE exists because of a CVE-2023-28617 security regression for the emacs package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2491**	N/A	O-RED-ENTE-020623/5641
N/A	17-May-2023	7.5	A vulnerability was found in the libreswan library. This security issue occurs when an IKEv1 Aggressive Mode packet is received with only unacceptable crypto algorithms, and the response packet is not sent	N/A	O-RED-ENTE-020623/5642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with a zero responder SPI. When a subsequent packet is received where the sender reuses the libreswan responder SPI as its own initiator SPI, the pluto daemon state machine crashes. No remote code execution is possible. This CVE exists because of a CVE-2023-30570 security regression for libreswan package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2. **CVE ID : CVE-2023-2295**		
Vendor: tandd					
Product: rtr-5w_firmware					
Affected Version(s): *					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-RTR--020623/5643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-RTR--020623/5644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-RTR--020623/5645

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-RTR--020623/5646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**		
Product: tr-71w_firmware					
Affected Version(s): *					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions),	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-TR-7-020623/5647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-TR-7-020623/5648

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-TR-7-020623/5649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions).	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-TR-7-020623/5650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-23545		
Product: tr-72w_firmware					
Affected Version(s): *					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-TR-7-020623/5651

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-TR-7-020623/5652
Improper Neutralization of	23-May-2023	5.4	Client-side enforcement of server-side security	https://www.monitoring.especmic.co.jp/	O-TAN-TR-7-020623/5653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**	post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-	O-TAN-TR-7-020623/5654

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**	22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	
Product: wdr-3_firmware					
Affected Version(s): *					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-	O-TAN-WDR--020623/5655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**	12N, https://www.tandd.com/news/detail.html?id=780	
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-WDR--020623/5656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-WDR--020623/5657

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-WDR--020623/5658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**		
Product: wdr-7_firmware					
Affected Version(s): *					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-WDR--020623/5659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-WDR--020623/5660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-27387**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-WDR--020623/5661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**		
Missing Authentication for Critical Function	23-May-2023	5.3	Missing authentication for critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-WDR--020623/5662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**		
Product: ws-2_firmware					
Affected Version(s): *					
Improper Authentication	23-May-2023	9.8	Improper authentication vulnerability in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to login to the product as a registered user. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions,	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-WS-2-020623/5663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and TEU-12N all firmware versions). **CVE ID : CVE-2023-27388**		
Cross-Site Request Forgery (CSRF)	23-May-2023	8.8	Cross-site request forgery (CSRF) in T&D Corporation and ESPEC MIC CORP. data logger products allows a remote unauthenticated attacker to conduct an arbitrary operation by having a logged-in user view a malicious page. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions).	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-WS-2-020623/5664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2023-27387		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-May-2023	5.4	Client-side enforcement of server-side security issue exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may lead to an arbitrary script execution on a logged-in user's web browser. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-22654**	https://www.monitoring.especmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	O-TAN-WS-2-020623/5665
Missing Authentica	23-May-2023	5.3	Missing authentication for	https://www.monitoring.es	O-TAN-WS-2-020623/5666

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
tion for Critical Function			critical function exists in T&D Corporation and ESPEC MIC CORP. data logger products, which may allow a remote unauthenticated attacker to alter the product settings without authentication. Affected products and versions are as follows: T&D Corporation data logger products (TR-71W/72W all firmware versions, RTR-5W all firmware versions, WDR-7 all firmware versions, WDR-3 all firmware versions, and WS-2 all firmware versions), and ESPEC MIC CORP. data logger products (RT-12N/RS-12N all firmware versions, RT-22BN all firmware versions, and TEU-12N all firmware versions). **CVE ID : CVE-2023-23545**	pecmic.co.jp/post/VulnerabilityInRT-12N_RS-12N_RT-22BNandTEU-12N, https://www.tandd.com/news/detail.html?id=780	
Vendor: Tenda					
Product: ac5_firmware					
Affected Version(s): 15.03.06.28					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-May-2023	9.8	Tenda AC5 router V15.03.06.28 was discovered to contain a remote code execution (RCE) vulnerability via the Mac parameter at ip/goform/WriteFacMac. **CVE ID : CVE-2023-31587**	https://www.tenda.com.cn/product/AC5.html	O-TEN-AC5_-020623/5667
Vendor: totolink					
Product: a3300r_firmware					
Affected Version(s): 17.0.0cu.557					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-May-2023	9.8	TOTOLINK A3300R v17.0.0cu.557 is vulnerable to Command Injection. **CVE ID : CVE-2023-31729**	N/A	O-TOT-A330-020623/5668
Product: cp300\+_firmware					
Affected Version(s): 5.2cu.7594_b20200910					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-May-2023	9.8	A command injection vulnerability in the hostTime parameter in the function NTPSyncWithHostof TOTOLINK CP300+ V5.2cu.7594_B20200910 allows attackers to execute arbitrary	N/A	O-TOT-CP30-020623/5669

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			commands via a crafted http packet. **CVE ID : CVE-2023-31856**		
Product: n200re_firmware					
Affected Version(s): 9.3.5u.6255_b20211224					
Password in Configuration File	18-May-2023	5.5	A vulnerability classified as problematic has been found in TOTOLINK N200RE 9.3.5u.6255_B20211224. Affected is an unknown function of the file /squashfs-root/etc_ro/custom.conf of the component Telnet Service. The manipulation leads to password in configuration file. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used. VDB-229374 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way. **CVE ID : CVE-2023-2790**	N/A	O-TOT-N200-020623/5670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Tp-link					
Product: archer_vr1600v_firmware					
Affected Version(s): * Up to (including) 0.1.0_0.9.1_v5006.0_build_200810_rel.53181n					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-May-2023	6.7	A command injection vulnerability exists in the administrative web portal in TP-Link Archer VR1600V devices running firmware Versions <= 0.1.0. 0.9.1 v5006.0 Build 220518 Rel.32480n which allows remote attackers, authenticated to the administrative web portal as an administrator user to open an operating system level shell via the 'X_TP_IfName' parameter. **CVE ID : CVE-2023-31756**	N/A	O-TP--ARCH-020623/5671
Product: tl-wpa4530_kit_firmware					
Affected Version(s): 161115					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	8.8	TP-Link TL-WPA4530 KIT V2 (EU)_170406 and V2 (EU)_161115 is vulnerable to Command Injection via _httpRpmPlcDeviceAdd. **CVE ID : CVE-2023-31700**	N/A	O-TP--TL-W-020623/5672

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	8.8	TP-Link TL-WPA4530 KIT V2 (EU)_170406 and V2 (EU)_161115 is vulnerable to Command Injection via _httpRpmPlcDeviceRemove. **CVE ID : CVE-2023-31701**	N/A	O-TP--TL-W-020623/5673
Affected Version(s): 170406					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	8.8	TP-Link TL-WPA4530 KIT V2 (EU)_170406 and V2 (EU)_161115 is vulnerable to Command Injection via _httpRpmPlcDeviceAdd. **CVE ID : CVE-2023-31700**	N/A	O-TP--TL-W-020623/5674
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-May-2023	8.8	TP-Link TL-WPA4530 KIT V2 (EU)_170406 and V2 (EU)_161115 is vulnerable to Command Injection via _httpRpmPlcDeviceRemove. **CVE ID : CVE-2023-31701**	N/A	O-TP--TL-W-020623/5675