National Critical Information Infrastructure Protection Centre
Common Vulnerabilities and Exposures (CVE) Report
16 - 31 Dec 2022 Vol. 09 No. 24

Table of Content

Vendor	Product	Page Number
Application		
10web	photo_gallery	1
abacus-ext-cmdline_project	abacus-ext-cmdline	1
Adobe	campaign	1
	experience_manager	2
	experience_manager_cloud_service	17
	illustrator	30
aerocms_project	aerocms	33
alinto	sogo	34
Ampache	ampache	35
Apache	apache-airflow-providers-apache-hive	36
	helix	36
	karaf	37
	shardingsphere	39
	traffic_server	39
	zeppelin	42
apiman	apiman	42
auth0	jsonwebtoken	43
Autodesk	dwg_trueview	46
	maya	46
auto_upload_images_project	auto_upload_images	47
axiosys	bento4	48
beardev	joomsport	49
bigbluebutton	bigbluebutton	49
Blogengine	blogengine.net	55
bostonsleep	slice	56

Vendor	Product	Page Number
Brave	brave	56
Broadcom	symantec_identity_governance_and_administration	58
cedcommerce	smsa_shipping_for_woocommerce	59
	wholesale_market_for_woocommerce	60
clickstudios	passwordstate	61
Codeigniter	codeigniter	70
codelights-shortcodes-and-widgets_project	codelights-shortcodes-and-widgets	71
collective.contact.widget_project	collective.contact.widget	71
contec	conprosys_hmi_system	72
covid-19_directory_on_vaccination_system_project	covid-19_directory_on_vaccination_system	73
crmx_project	crmx	73
daloradius	daloradius	74
datadoghq	guarddog	74
deltaww	dopsoft	76
devolutions	remote_desktop_manager	76
django-openipam_project	django-openipam	77
django_terms_and_conditions_project	django_terms_and_conditions	77
drachtio	drachtio-server	78
easy-static-server_project	easy-static-server	79
emby	emby	80
employee_performance_evaluation_system_project	employee_performance_evaluation_system	80
entropymine	deark	80
ep-3bookingsystem	ep-3_bookingsystem	81
external_media_project	external_media	81
exuberant_ctags_project	exuberant_ctags	82

Vendor	Product	Page Number
F-secure	safe	82
Ffmpeg	ffmpeg	83
Flatpress	flatpress	83
freedom	securedrop	84
Genetechsolutions	pie_register	85
ghinstallation_project	ghinstallation	85
ghost	ghost	86
GNU	grub2	87
grafana	enterprise_metrics	87
hcltech	bigfix_platform	89
	bigfix_server_automation	90
	bigfix_webui	90
	digital_experience	91
	hcl_digital_experience	92
hcltechsw	bigfix_insights_for_vulnerability_remediation	92
hutool	hutool	93
IBM	cognos_analytics	94
	domino	98
	financial_transaction_manager	101
	notes	101
	security_guardium	106
	security_verify_governance	107
	spectrum_control	109
	spectrum_scale	109
	urbancode_deploy	109
	vios	112
ikus-soft	rdiffweb	114
inex	ixp_manager	115
inhabit	move_crm	116
iofinnet	tss-lib	116
Isode	m-vault	117
jacic	electronic_bidding_core_system	117

Vendor	Product	Page Number
jegtheme	jeg_elementor_kit	119
Jetbrains	intellij_idea	120
joget	joget_dx	120
json5	json5	121
Linuxfoundation	cortex	123
liquidjs	liquidjs	126
lite-server_project	lite-server	126
Mediawiki	semantic_drilldown	127
Microfocus	groupwise	127
Microweber	microweber	128
mind-map_project	mind-map	129
mingsoft	mcms	129
Misp-project	malware_information_sharing_platform	130
Mozilla	firefox	130
	firefox_esr	163
	firefox_focus	186
	thunderbird	187
	vpn	213
Mutiny	mutiny	213
nbnbk_project	nbnbk	213
ndk-design	ndkadvancedcustomizationfields	214
Netapp	oncommand_insight	214
noorsplugin	checkout_for_paypal	215
	easy_video_player	215
	responsive_lightbox2	216
	wp_stripe_checkout	216
oc-server3_project	oc-server3	216
Omron	cx-drive	219
Open-emr	openemr	219
openimageio	openimageio	220
openimageio_project	openimageio	221
Openstack	kolla	230

Vendor	Product	Page Number
Otrs	otrs	231
p4_project	p4	233
patchelf_project	patchelf	233
pdftojson_project	pdftojson	234
Pfsense	pfblockerng	234
pi-hole	adminlte	235
pig-vector_project	pig-vector	236
pivotal_software	concourse	236
pluginus	inpost_gallery	237
popup_manager_project	popup_manager	237
Poweriso	poweriso	238
properfraction	profilepress	239
Python	setuptools	240
pythoncharmers	python-future	241
Redhat	openstack	241
	satellite	241
retra-system_project	retra-system	243
rockoa	xinhu	243
ruoyi_project	ruoyi	243
safe-eval_project	safe-eval	244
Samba	ppp	245
search	docconv	246
shoplazza	lifestyle	246
silverwaregames	silverwaregames	250
simmeth	lieferantenmanager	251
smoothiecharts	smoothie_charts	253
snipeitapp	snipe-it	253
softr	softr	254
Solarwinds	serv-u	254
	solarwinds_platform	255
sslh_project	sslh	256
starter-public-edition-4_project	starter-public-edition-4	256

Vendor	Product	Page Number
tatoeba	tatoeba2	257
teluu	pjsip	258
thinkphp	thinkphp	258
tjws2_project	tjws2	259
toto_project	toto	260
trellix	endpoint_security	261
tum	ogc_web_feature_service	261
typora	typora	262
ubi_reader_project	ubi_reader	262
ucf	materia	263
ultimatemember	jobboardwp	264
usememos	memos	264
vms-studio	quizlord	268
Vmware	vrealize_operations	268
Wbce	wbce_cms	269
wfs	heaven_burns_red	270
wheel_project	wheel	270
wp-ban_project	wp-ban	270
wp-english-wp-admin_project	wp-english-wp-admin	271
wphowto	flowplayer_video_player	272
	videojs_html5_player	272
wpvar	wp_shamsi	273
wpwax	directorist	273
xml-rpc.net_project	xml-rpc.net	273
Zenphoto	Zenphoto	274
znote	znote	274
Zohocorp	manageengine_device_control_plus	275
Hardware		
AMD	amd64	276
Buffalo	wcr-1166ds	277
	wex-1800ax4	279
	wex-1800ax4ea	281

Vendor	Product	Page Number
Buffalo	wsr-2533dhp	283
	wsr-2533dhp2	285
	wsr-2533dhp3	287
	wsr-2533dhpl	290
	wsr-2533dhpl2	292
	wsr-2533dhpls	295
	wsr-3200ax4b	297
	wsr-3200ax4s	300
	wsr-a2533dhp2	303
	wsr-a2533dhp3	305
Dataprobe	iboot-pdu4-n20	308
	iboot-pdu4a-n15	311
	iboot-pdu4a-n20	313
	iboot-pdu4sa-n15	316
	iboot-pdu4sa-n20	319
	iboot-pdu8a-2n15	321
	iboot-pdu8a-2n20	324
	iboot-pdu8a-n15	326
	iboot-pdu8a-n20	329
	iboot-pdu8sa-2n15	332
	iboot-pdu8sa-n15	334
	iboot-pdu8sa-n20	337
Dlink	dap-2310	340
	dap-2330	340
	dap-2360	341
	dap-2553	342
	dap-2660	342
	dap-2690	343
	dap-2695	344
	dap-3320	344
	dap-3662	345
	dir-846	346

Vendor	Product	Page Number
Dlink	dir-869	346
	dir-869ax	346
Hikvision	ds-3wf01c-2n\/o	347
	ds-3wf0ac-2nt	347
Microchip	bm64	348
	bm70	348
	bm71	350
	bm77	352
	bm78	352
	bm83	354
	is1870	356
	is1871	357
	pic32cx1012bz25048	358
	pic_lightblue_explorer_demo	359
	rn4678	361
	rn4870	362
	rn4871	363
	wbz451	365
Netgear	nighthawk_ax11000	366
	nighthawk_ax1800	366
	nighthawk_ax2400	367
	nighthawk_ax3000	367
	nighthawk_ax5400	367
	nighthawk_ax6000	368
	rax30	368
	wnr2000	369
	xwn5001	370
Nokia	fastmile	370
paxtechnology	a930	371
Rockwellautomation	compactlogix_5370	372
	compactlogix_5380	373
	compactlogix_5480	373

Vendor	Product	Page Number
Rockwellautomation	compactlogix_5580	374
	compact_guardlogix_5370	374
	compact_guardlogix_5380	375
	controllogix_5570	376
	controllogix_5570_redundancy	376
	guardlogix_5570	376
	guardlogix_5580	377
	micrologix_1100	377
	micrologix_1400	379
	micrologix_1400-a	380
	micrologix_1400-b	380
	micrologix_1400-c	381
Sharp	bp-30c25	382
	bp-30c25t	382
	bp-30c25y	383
	bp-30c25z	384
	bp-30m28	384
	bp-30m28t	385
	bp-30m31	386
	bp-30m31t	386
	bp-30m35	387
	bp-30m35t	388
	bp-50c26	388
	bp-50c31	389
	bp-50c36	390
	bp-50c45	390
	bp-50c55	391
	bp-50c65	392
	bp-50m26	392
	bp-50m31	393
	bp-50m36	394
	bp-50m45	394

Vendor	Product	Page Number
Sharp	bp-50m50	395
	bp-50m55	396
	bp-55c26	396
	bp-60c31	397
	bp-60c36	398
	bp-60c45	398
	bp-70c31	399
	bp-70c36	400
	bp-70c45	400
	bp-70c55	401
	bp-70c65	402
	bp-70m31	402
	bp-70m36	403
	bp-70m45	404
	bp-70m55	404
	bp-70m65	405
	bp-70m75	406
	bp-70m90	406
	mx-2630n	407
	mx-2651	408
	mx-3050n	408
	mx-3050n_a	409
	mx-3050v	410
	mx-3050v_a	410
	mx-3051	411
	mx-3060n	412
	mx-3060v	412
	mx-3061	413
	mx-3061s	414
	mx-3070n	414
	mx-3070n_a	415
	mx-3070v	416

Vendor	Product	Page Number
Sharp	mx-3070v_a	416
	mx-3071	417
	mx-3071s	418
	mx-3550n	418
	mx-3550v	419
	mx-3551	420
	mx-3560n	420
	mx-3560v	421
	mx-3561	422
	mx-3561s	422
	mx-3570n	423
	mx-3570v	424
	mx-3571	424
	mx-3571s	425
	mx-4050n	426
	mx-4050v	426
	mx-4051	427
	mx-4060n	428
	mx-4060v	428
	mx-4061	429
	mx-4061s	430
	mx-4070n	430
	mx-4070n_a	431
	mx-4070v	432
	mx-4070v_a	432
	mx-4071	433
	mx-4071s	434
	mx-5050n	434
	mx-5050v	435
	mx-5051	436
	mx-5070n	436
	mx-5070v	437

Vendor	Product	Page Number
Sharp	mx-5071	438
	mx-5071s	438
	mx-6050n	439
	mx-6050v	440
	mx-6051	440
	mx-6070n	441
	mx-6070n_a	442
	mx-6070v	442
	mx-6070v_a	443
	mx-6071	444
	mx-6071s	444
	mx-6580n	445
	mx-7081	446
	mx-7090n	446
	mx-7580n	447
	mx-8081	448
	mx-8090n	448
	mx-b355w	449
	mx-b355wt	450
	mx-b355wz	450
	mx-b356w	451
	mx-b356wh	452
	mx-b376w	452
	mx-b376wh	453
	mx-b455w	454
	mx-b455wt	454
	mx-b455wz	455
	mx-b456w	456
	mx-b456wh	456
	mx-b476w	457
	mx-b476wh	458
	mx-c303	458

Vendor	Product	Page Number
Sharp	mx-c303w	459
	mx-c303wh	460
	mx-c304	460
	mx-c304w	461
	mx-c304wh	462
	mx-m1056	462
	mx-m1206	463
	mx-m2630	464
	mx-m2630_a	464
	mx-m2651	465
	mx-m3050	466
	mx-m3050_a	466
	mx-m3051	467
	mx-m3070	468
	mx-m3070_a	468
	mx-m3071	469
	mx-m3071s	470
	mx-m3550	470
	mx-m3551	471
	mx-m3570	472
	mx-m3571	472
	mx-m3571s	473
	mx-m4050	474
	mx-m4051	474
	mx-m4070	475
	mx-m4070_a	476
	mx-m4071	476
	mx-m4071s	477
	mx-m5050	478
	mx-m5051	478
	mx-m5070	479
	mx-m5071	480

Vendor	Product	Page Number
Sharp	mx-m5071s	480
	mx-m6050	481
	mx-m6051	482
	mx-m6070	482
	mx-m6070_a	483
	mx-m6071	484
	mx-m6071s	484
	mx-m6570	485
	mx-m7570	486
	mx-m905	486
sick	sim2000st	487
Tenda	ac10	488
	f1203	488
	i22	493
Tp-link	tl-wa7510n_v1	494
	tl-wa801n	494
	tl-wa801nd_v1	494
	tl-wa901n	495
	tl-wa901nd_v1	495
	tl-wa901nd_v2	496
	tl-wr1043nd_v1	496
	tl-wr740n_v1	496
	tl-wr740n_v2	497
	tl-wr741nd_v1	497
	tl-wr741nd_v2	497
	tl-wr743nd_v1	498
	tl-wr841n	498
	tl-wr841nd_v7	499
	tl-wr940n_v4	499
	tl-wr941nd_v2	499
	tl-wr941nd_v3	500
	tl-wr941nd_v4	500

Vendor	Product	Page Number
Zyxel	nbg7510	501
Operating System		
Apple	iphone_os	501
	macos	501
Buffalo	wcr-1166ds_firmware	505
	wex-1800ax4ea_firmware	507
	wex-1800ax4_firmware	509
	wsr-2533dhp2_firmware	510
	wsr-2533dhp3_firmware	513
	wsr-2533dhpl2_firmware	516
	wsr-2533dhpls_firmware	518
	wsr-2533dhpl_firmware	521
	wsr-2533dhp_firmware	523
	wsr-3200ax4b_firmware	525
	wsr-3200ax4s_firmware	528
	wsr-a2533dhp2_firmware	530
	wsr-a2533dhp3_firmware	533
contiki-ng	contiki-ng	536
Dataprobe	iboot-pdu4-n20_firmware	537
	iboot-pdu4a-n15_firmware	540
	iboot-pdu4a-n20_firmware	542
	iboot-pdu4sa-n15_firmware	545
	iboot-pdu4sa-n20_firmware	548
	iboot-pdu8a-2n15_firmware	550
	iboot-pdu8a-2n20_firmware	553
	iboot-pdu8a-n15_firmware	556
	iboot-pdu8a-n20_firmware	558
	iboot-pdu8sa-2n15_firmware	561
	iboot-pdu8sa-n15_firmware	564
	iboot-pdu8sa-n20_firmware	566
Dlink	dap-2310_firmware	569
	dap-2330_firmware	570

Vendor	Product	Page Number
Dlink	dap-2360_firmware	570
	dap-2553_firmware	571
	dap-2660_firmware	572
	dap-2690_firmware	572
	dap-2695_firmware	573
	dap-3320_firmware	574
	dap-3662_firmware	575
	dir-846_firmware	576
	dir-869ax_firmware	577
	dir-869_firmware	577
Google	android	577
Hikvision	ds-3wf01c-2n\/o_firmware	643
	ds-3wf0ac-2nt_firmware	644
Huawei	emui	644
	harmonyos	657
IBM	aix	665
	i	674
	linux_on_zseries	679
Juniper	junos	680
	junos_os_evolved	681
linaro	op-tee	683
Linux	linux_kernel	684
Microchip	bm64_firmware	692
	bm70_firmware	693
	bm71_firmware	695
	bm77_firmware	696
	bm78_firmware	697
	bm83_firmware	699
	is1870_firmware	700
	is1871_firmware	702
	pic32cx1012bz25048_firmware	703
	pic_lightblue_explorer_demo_firmware	704

Vendor	Product	Page Number
Microchip	rn4678_firmware	706
	rn4870_firmware	706
	rn4871_firmware	708
	wbz451_firmware	710
Microsoft	windows	710
Netgear	nighthawk_ax11000_firmware	717
	nighthawk_ax1800_firmware	717
	nighthawk_ax2400_firmware	717
	nighthawk_ax3000_firmware	718
	nighthawk_ax5400_firmware	718
	nighthawk_ax6000_firmware	719
	rax30_firmware	719
	wnr2000_firmware	720
	xwn5001_firmware	721
Nokia	fastmile_firmware	721
Oracle	solaris	722
paxtechnology	paydroid	722
Redhat	enterprise_linux	724
Rockwellautomation	compactlogix_5370_firmware	724
	compactlogix_5380_firmware	725
	compactlogix_5480_firmware	725
	compactlogix_5580_firmware	726
	compact_guardlogix_5370_firmware	726
	compact_guardlogix_5380_firmware	727
	controllogix_5570_firmware	728
	controllogix_5570_redundancy_firmware	728
	guardlogix_5570_firmware	728
	guardlogix_5580_firmware	729
	micrologix_1100_firmware	729
	micrologix_1400-a_firmware	730
	micrologix_1400-b_firmware	731
	micrologix_1400-c_firmware	732

Vendor	Product	Page Number
Rockwellautomation	micrologix_1400_firmware	732
Sharp	bp-30c25t_firmware	734
	bp-30c25y_firmware	734
	bp-30c25z_firmware	735
	bp-30c25_firmware	736
	bp-30m28t_firmware	736
	bp-30m28_firmware	737
	bp-30m31t_firmware	738
	bp-30m31_firmware	738
	bp-30m35t_firmware	739
	bp-30m35_firmware	740
	bp-50c26_firmware	740
	bp-50c31_firmware	741
	bp-50c36_firmware	742
	bp-50c45_firmware	742
	bp-50c55_firmware	743
	bp-50c65_firmware	744
	bp-50m26_firmware	744
	bp-50m31_firmware	745
	bp-50m36_firmware	746
	bp-50m45_firmware	746
	bp-50m50_firmware	747
	bp-50m55_firmware	748
	bp-55c26_firmware	748
	bp-60c31_firmware	749
	bp-60c36_firmware	750
	bp-60c45_firmware	750
	bp-70c31_firmware	751
	bp-70c36_firmware	752
	bp-70c45_firmware	752
	bp-70c55_firmware	753
	bp-70c65_firmware	754

Vendor	Product	Page Number
Sharp	bp-70m31_firmware	754
	bp-70m36_firmware	755
	bp-70m45_firmware	756
	bp-70m55_firmware	756
	bp-70m65_firmware	757
	bp-70m75_firmware	758
	bp-70m90_firmware	758
	mx-2630n_firmware	759
	mx-2651_firmware	760
	mx-3050n_a_firmware	760
	mx-3050n_firmware	761
	mx-3050v_a_firmware	762
	mx-3050v_firmware	762
	mx-3051_firmware	763
	mx-3060n_firmware	764
	mx-3060v_firmware	764
	mx-3061s_firmware	765
	mx-3061_firmware	766
	mx-3070n_a_firmware	766
	mx-3070n_firmware	767
	mx-3070v_a_firmware	768
	mx-3070v_firmware	768
	mx-3071s_firmware	769
	mx-3071_firmware	770
	mx-3550n_firmware	770
	mx-3550v_firmware	771
	mx-3551_firmware	772
	mx-3560n_firmware	772
	mx-3560v_firmware	773
	mx-3561s_firmware	774
	mx-3561_firmware	774
	mx-3570n_firmware	775

Vendor	Product	Page Number
Sharp	mx-3570v_firmware	776
	mx-3571s_firmware	776
	mx-3571_firmware	777
	mx-4050n_firmware	778
	mx-4050v_firmware	778
	mx-4051_firmware	779
	mx-4060n_firmware	780
	mx-4060v_firmware	780
	mx-4061s_firmware	781
	mx-4061_firmware	782
	mx-4070n_a_firmware	782
	mx-4070n_firmware	783
	mx-4070v_a_firmware	784
	mx-4070v_firmware	784
	mx-4071s_firmware	785
	mx-4071_firmware	786
	mx-5050n_firmware	786
	mx-5050v_firmware	787
	mx-5051_firmware	788
	mx-5070n_firmware	788
	mx-5070v_firmware	789
	mx-5071s_firmware	790
	mx-5071_firmware	790
	mx-6050n_firmware	791
	mx-6050v_firmware	792
	mx-6051_firmware	792
	mx-6070n_a_firmware	793
	mx-6070n_firmware	794
	mx-6070v_a_firmware	794
	mx-6070v_firmware	795
	mx-6071s_firmware	796
	mx-6071_firmware	796

Vendor	Product	Page Number
Sharp	mx-6580n_firmware	797
	mx-7081_firmware	798
	mx-7090n_firmware	798
	mx-7580n_firmware	799
	mx-8081_firmware	800
	mx-8090n_firmware	800
	mx-b355wt_firmware	801
	mx-b355wz_firmware	802
	mx-b355w_firmware	802
	mx-b356wh_firmware	803
	mx-b356w_firmware	804
	mx-b376wh_firmware	804
	mx-b376w_firmware	805
	mx-b455wt_firmware	806
	mx-b455wz_firmware	806
	mx-b455w_firmware	807
	mx-b456wh_firmware	808
	mx-b456w_firmware	808
	mx-b476wh_firmware	809
	mx-b476w_firmware	810
	mx-c303wh_firmware	810
	mx-c303w_firmware	811
	mx-c303_firmware	812
	mx-c304wh_firmware	812
	mx-c304w_firmware	813
	mx-c304_firmware	814
	mx-m1056_firmware	814
	mx-m1206_firmware	815
	mx-m2630_a_firmware	816
	mx-m2630_firmware	816
	mx-m2651_firmware	817
	mx-m3050_a_firmware	818

Vendor	Product	Page Number
Sharp	mx-m3050_firmware	818
	mx-m3051_firmware	819
	mx-m3070_a_firmware	820
	mx-m3070_firmware	820
	mx-m3071s_firmware	821
	mx-m3071_firmware	822
	mx-m3550_firmware	822
	mx-m3551_firmware	823
	mx-m3570_firmware	824
	mx-m3571s_firmware	824
	mx-m3571_firmware	825
	mx-m4050_firmware	826
	mx-m4051_firmware	826
	mx-m4070_a_firmware	827
	mx-m4070_firmware	828
	mx-m4071s_firmware	828
	mx-m4071_firmware	829
	mx-m5050_firmware	830
	mx-m5051_firmware	830
	mx-m5070_firmware	831
	mx-m5071s_firmware	832
	mx-m5071_firmware	832
	mx-m6050_firmware	833
	mx-m6051_firmware	834
	mx-m6070_a_firmware	834
	mx-m6070_firmware	835
	mx-m6071s_firmware	836
	mx-m6071_firmware	836
	mx-m6570_firmware	837
	mx-m7570_firmware	838
	mx-m905_firmware	838
sick	sim2000_firmware	839

Vendor	Product	Page Number
Tenda	ac10_firmware	840
	f1203_firmware	840
	i22_firmware	845
Tp-link	tl-wa7510n_v1_firmware	846
	tl-wa801nd_v1_firmware	846
	tl-wa801n_firmware	846
	tl-wa901nd_v1_firmware	847
	tl-wa901nd_v2_firmware	847
	tl-wa901n_firmware	847
	tl-wr1043nd_v1_firmware	848
	tl-wr740n_v1_firmware	849
	tl-wr740n_v2_firmware	849
	tl-wr741nd_v1_firmware	849
	tl-wr741nd_v2_firmware	850
	tl-wr743nd_v1_firmware	850
	tl-wr841nd_v7_firmware	851
	tl-wr841n_firmware	851
	tl-wr940n_v4_firmware	851
	tl-wr941nd_v2_firmware	852
	tl-wr941nd_v3_firmware	852
	tl-wr941nd_v4_firmware	852
Zyxel	nbg7510_firmware	853

Common Vulnerabilities and Exposures (CVE) Report

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Application					
Vendor: 10web					
Product: photo_gallery					
Affected Version(s): * Up to (excluding) 1.8.3					
Cross-Site Request Forgery (CSRF)	19-Dec-2022	5.4	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control. **CVE ID : CVE-2022-4058**	N/A	A-10W-PHOT-090123/1
Vendor: abacus-ext-cmdline_project					
Product: abacus-ext-cmdline					
Affected Version(s): *					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	21-Dec-2022	9.8	All versions of package abacus-ext-cmdline are vulnerable to Command Injection via the execute function due to improper user-input sanitization. **CVE ID : CVE-2022-24431**	https://security.snyk.io/vuln/SNYK-JS-ABACUSEXTCMDLINE-3157950	A-ABA-ABAC-090123/2
Vendor: Adobe					
Product: campaign					
Affected Version(s): * Up to (excluding) 7.3.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	16-Dec-2022	6.5	Adobe Campaign version 7.3.1 (and earlier) and 8.3.9 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2022-42343**	https://helpx.adobe.com/security/products/campaign/apsb22-58.html	A-ADO-CAMP-090123/3
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.4.2					
Server-Side Request Forgery (SSRF)	16-Dec-2022	6.5	Adobe Campaign version 7.3.1 (and earlier) and 8.3.9 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2022-42343**	https://helpx.adobe.com/security/products/campaign/apsb22-58.html	A-ADO-CAMP-090123/4
Product: experience_manager					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2022.10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44510**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/5
Affected Version(s): * Up to (excluding) 6.5.15.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-30679**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/6
Improper Neutralization of Input During Web Page	16-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an	https://helpx.adobe.com/security/products/experience-manager/ap	A-ADO-EXPE-090123/7

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42360**	sb22-59.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-35694**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/8
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/9

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the victim's browser. **CVE ID : CVE-2022-42367**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-35696**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/10
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44510**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/11
Improper Neutralization of Input	16-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site	https://helpx.adobe.com/security/products/expe	A-ADO-EXPE-090123/12

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42366**	rience-manager/apsb22-59.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-35693**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/13
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/14

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the victim's browser. **CVE ID : CVE-2022-35695**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42345**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/15
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42346**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/16
Improper Neutralization of Input	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site	https://helpx.adobe.com/security/products/expe	A-ADO-EXPE-090123/17

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42348**	rience-manager/apsb22-59.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42349**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/18
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/19

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the victim's browser. **CVE ID : CVE-2022-42350**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42352**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/20
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42354**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/21
Improper Neutralization of Input	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site	https://helpx.adobe.com/security/products/expe	A-ADO-EXPE-090123/22

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42356**	rience-manager/apsb22-59.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42357**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/23
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/24

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the victim's browser. **CVE ID : CVE-2022-42362**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42365**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/25
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44462**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/26
Improper Neutralization of Input	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site	https://helpx.adobe.com/security/products/expe	A-ADO-EXPE-090123/27

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44463**	rience-manager/apsb22-59.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44465**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/28
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/29

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the victim's browser. **CVE ID : CVE-2022-44466**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44467**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/30
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44468**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/31
Improper Neutralization of Input	16-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site	https://helpx.adobe.com/security/products/expe	A-ADO-EXPE-090123/32

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44469**	rience-manager/apsb22-59.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44470**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/33
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/34

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			context of the victim's browser. **CVE ID : CVE-2022-44471**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44473**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/35
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44474**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/36
URL Redirection to Untrusted	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a URL Redirection to	https://helpx.adobe.com/security/products/expe	A-ADO-EXPE-090123/37

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2022-44488**	rience-manager/apsb22-59.html	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42364**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/38
Incorrect Authorization	16-Dec-2022	4.3	Adobe Experience Manager version 6.5.14 (and earlier) is affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to disclose low level confidentiality information. Exploitation of this	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/39

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			issue does not require user interaction. **CVE ID : CVE-2022-42351**		
Product: experience_manager_cloud_service					
Affected Version(s): * Up to (excluding) 2022.10.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-30679**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/40
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42360**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/41

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-35694**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/42
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42366**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/43
Improper Neutralization of Input During Web Page Generation	16-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/44

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-35696**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42367**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/45
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-35695**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/46

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42345**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/47
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42346**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/48
Improper Neutralization of Input During Web Page Generation	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/49

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42348**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42349**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/50
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42350**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/51

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42352**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/52
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42354**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/53
Improper Neutralization of Input During Web Page Generation	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/54

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42356**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42357**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/55
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42362**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/56

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42364**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/57
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-42365**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/58
Improper Neutralization of Input During Web Page Generation	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/59

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-35693**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44462**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/60
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44463**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/61

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44465**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/62
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44466**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/63
Improper Neutralization of Input During Web Page Generation	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/64

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44467**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44468**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/65
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44469**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/66

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44470**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/67
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44471**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/68
Improper Neutralization of Input During Web Page Generation	16-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/69

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44473**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. **CVE ID : CVE-2022-44474**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/70
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2022	5.4	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction. **CVE ID : CVE-2022-44488**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/71

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Dec-2022	4.3	Adobe Experience Manager version 6.5.14 (and earlier) is affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to disclose low level confidentiality information. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2022-42351**	https://helpx.adobe.com/security/products/experience-manager/apsb22-59.html	A-ADO-EXPE-090123/72
Product: illustrator					
Affected Version(s): * Up to (including) 26.5.1					
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44498**	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	A-ADO-ILLU-090123/73
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by	https://helpx.adobe.com/security/products/illust	A-ADO-ILLU-090123/74

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44499**	rator/apsb22-60.html	
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44500**	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	A-ADO-ILLU-090123/75
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	A-ADO-ILLU-090123/76

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44502**		
Affected Version(s): 27.0					
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44498**	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	A-ADO-ILLU-090123/77
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	A-ADO-ILLU-090123/78

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44499		
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44500**	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	A-ADO-ILLU-090123/79
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44502**	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	A-ADO-ILLU-090123/80
Vendor: aerocms_project					
Product: aerocms					
Affected Version(s): 0.0.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Dec-2022	7.5	AeroCMS v0.0.1 is vulnerable to Directory Traversal. The impact is: obtain sensitive information (remote). The component is: AeroCMS v0.0.1. **CVE ID : CVE-2022-46137**	N/A	A-AER-AERO-090123/81
Unrestricted Upload of File with Dangerous Type	16-Dec-2022	7.2	In AeroCms v0.0.1, there is an arbitrary file upload vulnerability at /admin/posts.php?source=edit_post , through which we can upload webshell and control the web server. **CVE ID : CVE-2022-46135**	N/A	A-AER-AERO-090123/82
Vendor: alinto					
Product: sogo					
Affected Version(s): * Up to (excluding) 5.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	A vulnerability was found in Alinto SOGo up to 5.7.1 and classified as problematic. Affected by this issue is the function _migrateMailIdentities of the file SoObjects/SOGo/SOGoUserDefaults.m of the component Identity Handler. The manipulation of the argument fullName leads to cross site scripting. The attack may be launched remotely. Upgrading to version 5.8.0 is able to address this issue. The	https://github.com/Alinto/sogo/commit/efac49ae91a4a325df9931e78e543f707a0f8e5e	A-ALI-SOGO-090123/83

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			name of the patch is efac49ae91a4a325df9931e78e543f707a0f8e5e. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-215960. **CVE ID : CVE-2022-4556**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	A vulnerability was found in Alinto SOGo up to 5.7.1. It has been classified as problematic. This affects an unknown part of the file SoObjects/SOGo/NSString+Utilities.m of the component Folder/Mail Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 5.8.0 is able to address this issue. The name of the patch is 1e0f5f00890f751e84d67be4f139dd7f00faa5f3. It is recommended to upgrade the affected component. The identifier VDB-215961 was assigned to this vulnerability. **CVE ID : CVE-2022-4558**	https://github.com/Alinto/sogo/commit/1e0f5f00890f751e84d67be4f139dd7f00faa5f3	A-ALI-SOGO-090123/84
Vendor: Ampache					
Product: ampache					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 5.5.6					
Unrestricted Upload of File with Dangerous Type	23-Dec-2022	8.8	Unrestricted Upload of File with Dangerous Type in GitHub repository ampache/ampache prior to 5.5.6. **CVE ID : CVE-2022-4665**	https://hunt r.dev/bounti es/5e7f3ecc-3b08-4e0e-8bf8-ae7ae22994 1f, https://gith ub.com/amp ache/ampac he/commit/ 8293fa86e5f 50a168b7f5 c892ffbd6aa 555134bd	A-AMP-AMPA-090123/85
Vendor: Apache					
Product: apache-airflow-providers-apache-hive					
Affected Version(s): * Up to (excluding) 5.0.0					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Dec-2022	9.8	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Software Foundation Apache Airflow Hive Provider.This issue affects Apache Airflow Hive Provider: before 5.0.0. **CVE ID : CVE-2022-46421**	https://lists. apache.org/t hread/09tw doyoybldlfj5 gvk0qswtofh 0rmp4, https://gith ub.com/apac he/airflow/ pull/28101	A-APA-APAC-090123/86
Product: helix					
Affected Version(s): From (including) 0.8.0 Up to (including) 1.0.4					
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2022	6.1	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Apache Software Foundation Apache Helix UI	https://lists. apache.org/t hread/lr74x txxbb1t3dfn 5qzzwl2xjr3 qlbmh	A-APA-HELI-090123/87

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			component.This issue affects Apache Helix all releases from 0.8.0 to 1.0.4. Solution: removed the the forward component since it was improper designed for UI embedding. User please upgrade to 1.1.0 to fix this issue. **CVE ID : CVE-2022-47500**		
Product: karaf					
Affected Version(s): * Up to (excluding) 4.3.8					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Dec-2022	9.8	This vulnerable is about a potential code injection when an attacker has control of the target LDAP server using in the JDBC JNDI URL. The function jaas.modules.src.main.java.porg.apache.karaf.jass.modules.jdbc.JDBCUtils#doCreateDatasource use InitialContext.lookup(jndiName) without filtering. An user can modify `options.put(JDBCUtils.DATASOURCE, "osgi:" + DataSource.class.getName());` to `options.put(JDBCUtils.DATASOURCE,"jndi:rmi://x.x.x.x:xxxx/Command");` in JdbcLoginModuleTest#setup. This is vulnerable to a remote code execution (RCE)	https://karaf.apache.org/security/cve-2022-40145.txt	A-APA-KARA-090123/88

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack when a configuration uses a JNDI LDAP data source URI when an attacker has control of the target LDAP server.This issue affects all versions of Apache Karaf up to 4.4.1 and 4.3.7. We encourage the users to upgrade to Apache Karaf at least 4.4.2 or 4.3.8 **CVE ID : CVE-2022-40145**		
Affected Version(s): From (including) 4.4.0 Up to (excluding) 4.4.2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-Dec-2022	9.8	This vulnerable is about a potential code injection when an attacker has control of the target LDAP server using in the JDBC JNDI URL. The function jaas.modules.src.main.java.porg.apache.karaf.jass.modules.jdbc.JDBCUtils#doCreateDatasource use InitialContext.lookup(jndiName) without filtering. An user can modify `options.put(JDBCUtils.DATASOURCE, "osgi:" + DataSource.class.getName());` to `options.put(JDBCUtils.DATASOURCE,"jndi:rmi://x.x.x.x:xxxx/Command");` in JdbcLoginModuleTest#setup. This is vulnerable to a remote	https://karaf.apache.org/security/cve-2022-40145.txt	A-APA-KARA-090123/89

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution (RCE) attack when a configuration uses a JNDI LDAP data source URI when an attacker has control of the target LDAP server.This issue affects all versions of Apache Karaf up to 4.4.1 and 4.3.7. We encourage the users to upgrade to Apache Karaf at least 4.4.2 or 4.3.8 **CVE ID : CVE-2022-40145**		
Product: shardingsphere					
Affected Version(s): * Up to (excluding) 5.3.0					
Incomplete Cleanup	22-Dec-2022	9.8	Apache ShardingSphere-Proxy prior to 5.3.0 when using MySQL as database backend didn't cleanup the database session completely after client authentication failed, which allowed an attacker to execute normal commands by constructing a special MySQL client. This vulnerability has been fixed in Apache ShardingSphere 5.3.0. **CVE ID : CVE-2022-45347**	https://lists.apache.org/thread/l5rz7j4rg10o7ywtgknh2f5hxnv6yw3l	A-APA-SHAR-090123/90
Product: traffic_server					
Affected Version(s): From (including) 8.0.0 Up to (excluding) 8.1.6					
Improper Check for	19-Dec-2022	7.5	Improper Check for Unusual or Exceptional	https://lists.apache.org/t	A-APA-TRAF-090123/91

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Unusual or Exceptional Conditions			Conditions vulnerability handling requests in Apache Traffic Server allows an attacker to crash the server under certain conditions. This issue affects Apache Traffic Server: from 8.0.0 through 9.1.3. **CVE ID : CVE-2022-32749**	hread/mrj2lg4s0hf027rk7gz8t7hbn9xpfg02	
Improper Check for Unusual or Exceptional Conditions	19-Dec-2022	5.3	Improper Check for Unusual or Exceptional Conditions vulnerability in handling the requests to Apache Traffic Server. This issue affects Apache Traffic Server 8.0.0 to 9.1.2. **CVE ID : CVE-2022-37392**	https://lists.apache.org/thread/mrj2lg4s0hf027rk7gz8t7hbn9xpfg02	A-APA-TRAF-090123/92
Affected Version(s): From (including) 8.0.0 Up to (including) 8.1.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	6.1	Improper Input Validation vulnerability for the xdebug plugin in Apache Software Foundation Apache Traffic Server can lead to cross site scripting and cache poisoning attacks.This issue affects Apache Traffic Server: 9.0.0 to 9.1.3. Users should upgrade to 9.1.4 or later versions. **CVE ID : CVE-2022-40743**	https://lists.apache.org/thread/mrj2lg4s0hf027rk7gz8t7hbn9xpfg02	A-APA-TRAF-090123/93
Affected Version(s): From (including) 9.0.0 Up to (excluding) 9.1.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Check for Unusual or Exceptional Conditions	19-Dec-2022	7.5	Improper Check for Unusual or Exceptional Conditions vulnerability handling requests in Apache Traffic Server allows an attacker to crash the server under certain conditions. This issue affects Apache Traffic Server: from 8.0.0 through 9.1.3. **CVE ID : CVE-2022-32749**	https://lists.apache.org/thread/mrj2lg4s0hf027rk7gz8t7hbn9xpfg02	A-APA-TRAF-090123/94
Improper Check for Unusual or Exceptional Conditions	19-Dec-2022	5.3	Improper Check for Unusual or Exceptional Conditions vulnerability in handling the requests to Apache Traffic Server. This issue affects Apache Traffic Server 8.0.0 to 9.1.2. **CVE ID : CVE-2022-37392**	https://lists.apache.org/thread/mrj2lg4s0hf027rk7gz8t7hbn9xpfg02	A-APA-TRAF-090123/95
Affected Version(s): From (including) 9.0.0 Up to (including) 9.1.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	6.1	Improper Input Validation vulnerability for the xdebug plugin in Apache Software Foundation Apache Traffic Server can lead to cross site scripting and cache poisoning attacks.This issue affects Apache Traffic Server: 9.0.0 to 9.1.3. Users should upgrade to 9.1.4 or later versions. **CVE ID : CVE-2022-40743**	https://lists.apache.org/thread/mrj2lg4s0hf027rk7gz8t7hbn9xpfg02	A-APA-TRAF-090123/96

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: zeppelin					
Affected Version(s): * Up to (excluding) 0.8.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	5.4	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache Zeppelin allows logged-in users to execute arbitrary javascript in other users' browsers. This issue affects Apache Zeppelin before 0.8.2. Users are recommended to upgrade to a supported version of Zeppelin. **CVE ID : CVE-2022-46870**	https://lists.apache.org/thread/gb1wdnrm1095xw6qznpsycfrht4lwbwc	A-APA-ZEPP-090123/97
Vendor: apiman					
Product: apiman					
Affected Version(s): From (including) 1.5.7 Up to (including) 2.2.3					
Incorrect Default Permissions	20-Dec-2022	6.5	Apiman 1.5.7 through 2.2.3.Final has insufficient checks for read permissions within the Apiman Manager REST API. The root cause of the issue is the Apiman project's accidental acceptance of a large contribution that was not fully compatible with the security model of Apiman versions before 3.0.0.Final. Because of this, 3.0.0.Final is not affected by the vulnerability.	https://www.apiman.io/blog/permissions-bypass-disclosure/	A-API-APIM-090123/98

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-47551		
Vendor: auth0					
Product: jsonwebtoken					
Affected Version(s): * Up to (including) 8.5.1					
Improper Input Validation	21-Dec-2022	9.8	node-jsonwebtoken is a JsonWebToken implementation for node.js. For versions `<= 8.5.1` of `jsonwebtoken` library, if a malicious actor has the ability to modify the key retrieval parameter (referring to the `secretOrPublicKey` argument from the readme link of the `jwt.verify()` function, they can write arbitrary files on the host machine. Users are affected only if untrusted entities are allowed to modify the key retrieval parameter of the `jwt.verify()` on a host that you control. This issue has been fixed, please update to version 9.0.0. **CVE ID : CVE-2022-23529**	https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3	A-AUT-JSON-090123/99
Use of a Broken or Risky Cryptographic Algorithm	22-Dec-2022	9.8	In versions `<=8.5.1` of `jsonwebtoken` library, lack of algorithm definition in the `jwt.verify()` function can lead to signature validation bypass due to defaulting to the `none` algorithm for	https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3	A-AUT-JSON-090123/100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			signature verification. Users are affected if you do not specify algorithms in the `jwt.verify()` function. This issue has been fixed, please update to version 9.0.0 which removes the default support for the none algorithm in the `jwt.verify()` method. There will be no impact, if you update to version 9.0.0 and you don't need to allow for the `none` algorithm. If you need 'none' algorithm, you have to explicitly specify that in `jwt.verify()` options. **CVE ID : CVE-2022-23540**		
N/A	22-Dec-2022	9.8	jsonwebtoken is an implementation of JSON Web Tokens. Versions `<= 8.5.1` of `jsonwebtoken` library can be misconfigured so that passing a poorly implemented key retrieval function referring to the `secretOrPublicKey` argument from the readme link will result in incorrect verification of tokens. There is a possibility of using a different algorithm and key combination in verification, other than the one that was used	https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3	A-AUT-JSON-090123/101

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to sign the tokens. Specifically, tokens signed with an asymmetric public key could be verified with a symmetric HS256 algorithm. This can lead to successful validation of forged tokens. If your application is supporting usage of both symmetric key and asymmetric key in jwt.verify() implementation with the same key retrieval function. This issue has been patched, please update to version 9.0.0. **CVE ID : CVE-2022-23541**		
Use of a Broken or Risky Cryptographic Algorithm	23-Dec-2022	8.1	Versions `<=8.5.1` of `jsonwebtoken` library could be misconfigured so that legacy, insecure key types are used for signature verification. For example, DSA keys could be used with the RS256 algorithm. You are affected if you are using an algorithm and a key type other than a combination listed in the GitHub Security Advisory as unaffected. This issue has been fixed, please update to version 9.0.0. This version validates for asymmetric key type and algorithm combinations. Please	https://github.com/auth0/node-jsonwebtoken/commit/e1fa9dcc12054a8681db4e6373da1b30cf7016e3	A-AUT-JSON-090123/102

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			refer to the above mentioned algorithm / key type combinations for the valid secure configuration. After updating to version 9.0.0, if you still intend to continue with signing or verifying tokens using invalid key type/algorithm value combinations, you'll need to set the `allowInvalidAsymmetricKeyTypes` option to `true` in the `sign()` and/or `verify()` functions. **CVE ID : CVE-2022-23539**		
Vendor: Autodesk					
Product: dwg_trueview					
Affected Version(s): 2023					
Uncontrolled Search Path Element	19-Dec-2022	7.8	DWG TrueViewTM 2023 version has a DLL Search Order Hijacking vulnerability. Successful exploitation by a malicious attacker could result in remote code execution on the target system. **CVE ID : CVE-2022-42945**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0024	A-AUT-DWG_-090123/103
Product: maya					
Affected Version(s): 2023					
Out-of-bounds Write	19-Dec-2022	7.8	A maliciously crafted X_B file when parsed through Autodesk Maya 2023 can be used to write beyond the	https://www.autodesk.com/trust/security-advisories/a	A-AUT-MAYA-090123/104

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allocated buffer. This vulnerability can lead to arbitrary code execution. **CVE ID : CVE-2022-42947**	dsk-sa-2022-0020	
Out-of-bounds Read	19-Dec-2022	7.1	Parsing a maliciously crafted X_B and PRT file can force Autodesk Maya 2023 to read beyond allocated buffer. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process. **CVE ID : CVE-2022-42946**	https://www.autodesk.com/trust/security-advisories/adsk-sa-2022-0020	A-AUT-MAYA-090123/105
Vendor: auto_upload_images_project					
Product: auto_upload_images					
Affected Version(s): * Up to (excluding) 3.3.1					
Cross-Site Request Forgery (CSRF)	21-Dec-2022	8.8	A vulnerability was found in Auto Upload Images up to 3.3.0 and classified as problematic. Affected by this issue is some unknown functionality of the file src/setting-page.php of the component Settings Handler. The manipulation leads to cross-site request forgery. The attack may be launched remotely. Upgrading to version 3.3.1 is able to address this issue. The name of the patch is 895770ee93887ec7842	https://github.com/airani/wp-auto-upload/commit/895770ee93887ec78429c78ffdfb865bee6f9436	A-AUT-AUTO-090123/106

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			9c78ffdfb865bee6f9436. It is recommended to upgrade the affected component. VDB-216482 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4633**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2022	6.1	A vulnerability has been found in Auto Upload Images up to 3.3.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 3.3.1 is able to address this issue. The name of the patch is 895770ee93887ec78429c78ffdfb865bee6f9436. It is recommended to upgrade the affected component. The identifier VDB-216481 was assigned to this vulnerability. **CVE ID : CVE-2022-4632**	https://github.com/airani/wp-auto-upload/commit/895770ee93887ec78429c78ffdfb865bee6f9436	A-AUT-AUTO-090123/107
Vendor: axiosys					
Product: bento4					
Affected Version(s): -					
Improper Restriction of Operations within the	17-Dec-2022	8.8	A vulnerability was found in Axiomatic Bento4. It has been rated as critical. Affected by this issue is	N/A	A-AXI-BENT-090123/108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			some unknown functionality of the component mp42aac. The manipulation leads to heap-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-216170 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4584**		
Vendor: beardev					
Product: joomsport					
Affected Version(s): * Up to (excluding) 5.2.8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Dec-2022	9.8	The JoomSport WordPress plugin before 5.2.8 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users **CVE ID : CVE-2022-4050**	N/A	A-BEA-JOOM-090123/109
Vendor: bigbluebutton					
Product: bigbluebutton					
Affected Version(s): * Up to (excluding) 2.4					
Exposure of Resource to Wrong Sphere	17-Dec-2022	7.5	BigBlueButton is an open source web conferencing system. Versions prior to 2.4-rc-6 are vulnerable to Insertion of Sensitive Information Into Sent Data. The moderators-	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GH	A-BIG-BIGB-090123/110

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			only webcams lock setting is not enforced on the backend, which allows an attacker to subscribe to viewers' webcams, even when the lock setting is applied. (The required streamId was being sent to all users even with lock setting applied). This issue is fixed in version 2.4-rc-6. There are no workarounds. **CVE ID : CVE-2022-23488**	SA-j5g3-f74q-rvfq	
Insufficient Verification of Data Authenticity	16-Dec-2022	4.3	BigBlueButton is an open source web conferencing system. Versions prior to 2.4-rc-6 are subject to Ineffective user bans. The attacker could register multiple users, and join the meeting with one of them. When that user is banned, they could still join the meeting with the remaining registered users from the same extId. This issue has been fixed by improving permissions such that banning a user removes all users related to their extId, including registered users that have not joined the meeting. This issue is patched in versions 2.4-rc-6 and	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-wxjp-h88g-7fqg	A-BIG-BIGB-090123/111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2.5-alpha-1. There are no workarounds. **CVE ID : CVE-2022-41961**		
Incorrect Authorization	16-Dec-2022	2.7	BigBlueButton is an open source web conferencing system. Versions prior to 2.4-rc-6, and 2.5-alpha-1 contain Incorrect Authorization for setting emoji status. A user with moderator rights can use the clear status feature to set any emoji status for other users. Moderators should only be able to set none as the status of other users. This issue is patched in 2.4-rc-6 and 2.5-alpha-1There are no workarounds. **CVE ID : CVE-2022-41962**	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-88qf-33qm-9mm7	A-BIG-BIGB-090123/112
Affected Version(s): * Up to (excluding) 2.4.0					
Incorrect Authorization	16-Dec-2022	4.3	BigBlueButton is an open source web conferencing system. Versions prior to 2.4.0 expose sensitive information to Unauthorized Actors. This issue affects meetings with polls, where the attacker is a meeting participant. Subscribing to the current-poll collection does not update the client UI, but does give the attacker access to	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-4qgc-xhw5-6qfg	A-BIG-BIGB-090123/113

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the contents of the collection, which include the individual poll responses. This issue is patched in version 2.4.0. There are no workarounds. **CVE ID : CVE-2022-23490**		
Affected Version(s): * Up to (excluding) 2.4.3					
Insufficient Verification of Data Authenticity	16-Dec-2022	4.3	BigBlueButton is an open source web conferencing system. Versions prior to 2.4.3, are subject to Insufficient Verification of Data Authenticity, resulting in Denial of Service. An attacker can make a Meteor call to `validateAuthToken` using a victim's userId, meetingId, and an invalid authToken. This forces the victim to leave the conference, because the resulting verification failure is also observed and handled by the victim's client. The attacker must be a participant in any meeting on the server. This issue is patched in version 2.4.3. There are no workarounds. **CVE ID : CVE-2022-41960**	N/A	A-BIG-BIGB-090123/114
Improper Preservation of	16-Dec-2022	3.1	BigBlueButton is an open source web conferencing system.	https://github.com/bigbluebutton/bi	A-BIG-BIGB-090123/115

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Permissions			Versions prior to 2.4.3 contain a whiteboard grace period that exists to handle delayed messages, but this grace period could be used by attackers to take actions in the few seconds after their access is revoked. The attacker must be a meeting participant. This issue is patched in version 2.4.3 an version 2.5-alpha-1 **CVE ID : CVE-2022-41963**	gbluebutton/security/advisories/GHSA-v6p9-926c-6qfp	
Affected Version(s): 2.4					
Exposure of Resource to Wrong Sphere	17-Dec-2022	7.5	BigBlueButton is an open source web conferencing system. Versions prior to 2.4-rc-6 are vulnerable to Insertion of Sensitive Information Into Sent Data. The moderators-only webcams lock setting is not enforced on the backend, which allows an attacker to subscribe to viewers' webcams, even when the lock setting is applied. (The required streamId was being sent to all users even with lock setting applied). This issue is fixed in version 2.4-rc-6. There are no workarounds.	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-j5g3-f74q-rvfq	A-BIG-BIGB-090123/116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23488		
Exposure of Sensitive Information to an Unauthorized Actor	16-Dec-2022	5.7	BigBlueButton is an open source web conferencing system. This vulnerability only affects release candidates of BigBlueButton 2.4. The attacker can start a subscription for poll results before starting an anonymous poll, and use this subscription to see individual responses in the anonymous poll. The attacker had to be a meeting presenter. This issue is patched in version 2.4.0. There are no workarounds. **CVE ID : CVE-2022-41964**	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-fgmj-rx7j-fqr4	A-BIG-BIGB-090123/117
Insufficient Verification of Data Authenticity	16-Dec-2022	4.3	BigBlueButton is an open source web conferencing system. Versions prior to 2.4-rc-6 are subject to Ineffective user bans. The attacker could register multiple users, and join the meeting with one of them. When that user is banned, they could still join the meeting with the remaining registered users from the same extId. This issue has been fixed by improving permissions such that banning a	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-wxjp-h88g-7fqg	A-BIG-BIGB-090123/118

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user removes all users related to their extId, including registered users that have not joined the meeting. This issue is patched in versions 2.4-rc-6 and 2.5-alpha-1. There are no workarounds. **CVE ID : CVE-2022-41961**		
Incorrect Authorization	16-Dec-2022	2.7	BigBlueButton is an open source web conferencing system. Versions prior to 2.4-rc-6, and 2.5-alpha-1 contain Incorrect Authorization for setting emoji status. A user with moderator rights can use the clear status feature to set any emoji status for other users. Moderators should only be able to set none as the status of other users. This issue is patched in 2.4-rc-6 and 2.5-alpha-1There are no workarounds. **CVE ID : CVE-2022-41962**	https://github.com/bigbluebutton/bigbluebutton/security/advisories/GHSA-88qf-33qm-9mm7	A-BIG-BIGB-090123/119
Vendor: Blogengine					
Product: blogengine.net					
Affected Version(s): 3.3.8.0					
Improper Limitation of a Pathname to a Restricted Directory	19-Dec-2022	7.2	An issue in the component BlogEngine/BlogEngine.NET/AppCode/Api/UploadController.cs of BlogEngine.NET v3.3.8.0 allows	https://github.com/BlogEngine/BlogEngine.NET/commit/7f927567db94462ffd37e128	A-BLO-BLOG-090123/120

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			attackers to execute arbitrary code via uploading a crafted PNG file. **CVE ID : CVE-2022-41418**	c0a53c11c1f81a8d	
Vendor: bostonsleep					
Product: slice					
Affected Version(s): * Up to (excluding) 84.2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-2022	6.1	A vulnerability, which was classified as problematic, was found in Boston Sleep slice up to 84.1.x. Affected is an unknown function of the component Layout Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 84.2.0 is able to address this issue. The name of the patch is 6523bb17d889e2ab13d767f38afefdb37083f1d0. It is recommended to upgrade the affected component. VDB-216174 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4588**	https://github.com/sleepepi/slice/commit/6523bb17d889e2ab13d767f38afefdb37083f1d0	A-BOS-SLIC-090123/121
Vendor: Brave					
Product: brave					
Affected Version(s): * Up to (excluding) 1.42.51					
N/A	24-Dec-2022	6.5	Brave Browser before 1.43.34 allowed a remote attacker to	https://github.com/brave/brave-	A-BRA-BRAV-090123/122

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service via a crafted HTML file that mentions an ipfs:// or ipns:// URL. This vulnerability is caused by an incomplete fix for CVE-2022-47933. **CVE ID : CVE-2022-47932**	core/commit/e73309665508c17e48a67e302d3ab02a38d3ef50, https://github.com/brave/brave-core/pull/14211	
N/A	24-Dec-2022	6.5	Brave Browser before 1.42.51 allowed a remote attacker to cause a denial of service via a crafted HTML file that references the IPFS scheme. This vulnerability is caused by an uncaught exception in the function ipfs::OnBeforeURLRequest_IPFSRedirectWork() in ipfs_redirect_network_delegate_helper.cc. **CVE ID : CVE-2022-47933**	https://github.com/brave/brave-core/commit/7ef8cb2f232abdf59ec9c3c99a086a14b972bc56, https://github.com/brave/brave-core/pull/13989	A-BRA-BRAV-090123/123
Affected Version(s): * Up to (excluding) 1.43.88					
N/A	24-Dec-2022	6.5	Brave Browser before 1.43.88 allowed a remote attacker to cause a denial of service in private and guest windows via a crafted HTML file that mentions an ipfs:// or ipns:// URL. This is caused by an incomplete fix for CVE-	https://github.com/brave/brave-core/pull/14313, https://github.com/brave/brave-core/commit/82d8e39043e691e0492519126437	A-BRA-BRAV-090123/124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2022-47932 and CVE-2022-47934. **CVE ID : CVE-2022-47934**	275511ee87e8	
Vendor: Broadcom					
Product: symantec_identity_governance_and_administration					
Affected Version(s): 14.3					
Improper Restriction of XML External Entity Reference	16-Dec-2022	8.8	An authenticated user can perform XML eXternal Entity injection in Management Console in Symantec Identity Manager 14.4 **CVE ID : CVE-2022-25628**	https://support.broadcom.com/external/content/SecurityAdvisories/0/21136	A-BRO-SYMA-090123/125
N/A	16-Dec-2022	6.7	An authenticated administrator who has physical access to the environment can carry out Remote Command Execution on Management Console in Symantec Identity Manager 14.4 **CVE ID : CVE-2022-25627**	https://support.broadcom.com/external/content/SecurityAdvisories/0/21136	A-BRO-SYMA-090123/126
Improper Authentication	16-Dec-2022	5.3	An unauthenticated user can access Identity Manager's management console specific page URLs. However, the system doesn't allow the user to carry out server side tasks without a valid web session. **CVE ID : CVE-2022-25626**	https://support.broadcom.com/external/content/SecurityAdvisories/0/21136	A-BRO-SYMA-090123/127
Affected Version(s): 14.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference	16-Dec-2022	8.8	An authenticated user can perform XML eXternal Entity injection in Management Console in Symantec Identity Manager 14.4 **CVE ID : CVE-2022-25628**	https://support.broadcom.com/external/content/SecurityAdvisories/0/21136	A-BRO-SYMA-090123/128
N/A	16-Dec-2022	6.7	An authenticated administrator who has physical access to the environment can carry out Remote Command Execution on Management Console in Symantec Identity Manager 14.4 **CVE ID : CVE-2022-25627**	https://support.broadcom.com/external/content/SecurityAdvisories/0/21136	A-BRO-SYMA-090123/129
Improper Authentication	16-Dec-2022	5.3	An unauthenticated user can access Identity Manager's management console specific page URLs. However, the system doesn't allow the user to carry out server side tasks without a valid web session. **CVE ID : CVE-2022-25626**	https://support.broadcom.com/external/content/SecurityAdvisories/0/21136	A-BRO-SYMA-090123/130
Vendor: cedcommerce					
Product: smsa_shipping_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.0.5					
Cross-Site Request Forgery (CSRF)	19-Dec-2022	6.5	The SMSA Shipping for WooCommerce WordPress plugin before 1.0.5 does not have authorisation and proper CSRF checks, as	N/A	A-CED-SMSA-090123/131

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			well as does not validate the file to be downloaded, allowing any authenticated users, such as subscriber to download arbitrary file from the server **CVE ID : CVE-2022-4107**		
Product: wholesale_market_for_woocommerce					
Affected Version(s): * Up to (excluding) 1.0.7					
Files or Directories Accessible to External Parties	19-Dec-2022	7.5	The Wholesale Market for WooCommerce WordPress plugin before 1.0.7 does not have authorisation check, as well as does not validate user input used to generate system path, allowing unauthenticated attackers to download arbitrary file from the server. **CVE ID : CVE-2022-4106**	N/A	A-CED-WHOL-090123/132
Affected Version(s): * Up to (excluding) 1.0.8					
Files or Directories Accessible to External Parties	19-Dec-2022	4.9	The Wholesale Market for WooCommerce WordPress plugin before 1.0.8 does not validate user input used to generate system path, allowing high privilege users such as admin to download arbitrary file from the server even when they should not be able to	N/A	A-CED-WHOL-090123/133

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(for example in multisite) **CVE ID : CVE-2022-4108**		
Vendor: clickstudios					
Product: passwordstate					
Affected Version(s): -					
Authentication Bypass by Assumed-Immutable Data	19-Dec-2022	7.5	A vulnerability classified as critical was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. This vulnerability affects unknown code of the component API. The manipulation leads to authentication bypass by assumed-immutable data. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216244. **CVE ID : CVE-2022-3875**	N/A	A-CLI-PASS-090123/134
Authorization Bypass Through User-Controlled Key	19-Dec-2022	6.5	A vulnerability, which was classified as problematic, has been found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. This issue affects some unknown processing of the file	N/A	A-CLI-PASS-090123/135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			/api/browserextension /UpdatePassword/ of the component API. The manipulation of the argument PasswordID leads to authorization bypass. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The identifier VDB-216245 was assigned to this vulnerability. **CVE ID : CVE-2022-3876**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	A vulnerability, which was classified as problematic, was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. Affected is an unknown function of the component URL Field Handler. The manipulation 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 upgrade the affected component. VDB-216246 is the identifier assigned to this vulnerability.	N/A	A-CLI-PASS-090123/136

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3877		
Affected Version(s): * Up to (excluding) 9.5					
Insufficiently Protected Credentials	19-Dec-2022	6.5	A vulnerability has been found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome and classified as problematic. This vulnerability affects unknown code. The manipulation leads to insufficiently protected credentials. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. VDB-216274 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4612**	N/A	A-CLI-PASS-090123/137
Incorrect Authorization	19-Dec-2022	6.5	A vulnerability was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome and classified as critical. This issue affects some unknown processing of the component Browser Extension Provisioning. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit	N/A	A-CLI-PASS-090123/138

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216275. **CVE ID : CVE-2022-4613**		
Use of a Broken or Risky Cryptographic Algorithm	19-Dec-2022	5.5	A vulnerability, which was classified as problematic, has been found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. Affected by this issue is some unknown functionality. The manipulation leads to risky cryptographic algorithm. 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-216272. **CVE ID : CVE-2022-4610**	N/A	A-CLI-PASS-090123/139
Use of Hard-coded Credentials	19-Dec-2022	5.3	A vulnerability, which was classified as problematic, was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. This affects an unknown part. The manipulation leads to hard-coded	N/A	A-CLI-PASS-090123/140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			credentials. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The identifier VDB-216273 was assigned to this vulnerability. **CVE ID : CVE-2022-4611**		
Affected Version(s): 9.5					
Insufficiently Protected Credentials	19-Dec-2022	6.5	A vulnerability has been found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome and classified as problematic. This vulnerability affects unknown code. The manipulation leads to insufficiently protected credentials. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. VDB-216274 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4612**	N/A	A-CLI-PASS-090123/141

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	19-Dec-2022	6.5	A vulnerability was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome and classified as critical. This issue affects some unknown processing of the component Browser Extension Provisioning. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216275. **CVE ID : CVE-2022-4613**	N/A	A-CLI-PASS-090123/142
Use of a Broken or Risky Cryptographic Algorithm	19-Dec-2022	5.5	A vulnerability, which was classified as problematic, has been found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. Affected by this issue is some unknown functionality. The manipulation leads to risky cryptographic algorithm. Local access is required to approach this attack. The exploit has been disclosed to the public and may be	N/A	A-CLI-PASS-090123/143

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			used. The identifier of this vulnerability is VDB-216272. **CVE ID : CVE-2022-4610**		
Use of Hard-coded Credentials	19-Dec-2022	5.3	A vulnerability, which was classified as problematic, was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. This affects an unknown part. The manipulation leads to hard-coded credentials. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The identifier VDB-216273 was assigned to this vulnerability. **CVE ID : CVE-2022-4611**	N/A	A-CLI-PASS-090123/144
Affected Version(s): 9.5.8.4					
Insufficiently Protected Credentials	19-Dec-2022	6.5	A vulnerability has been found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome and classified as problematic. This vulnerability affects unknown code. The manipulation leads to insufficiently protected credentials. The attack	N/A	A-CLI-PASS-090123/145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. VDB-216274 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4612**		
Incorrect Authorization	19-Dec-2022	6.5	A vulnerability was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome and classified as critical. This issue affects some unknown processing of the component Browser Extension Provisioning. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216275. **CVE ID : CVE-2022-4613**	N/A	A-CLI-PASS-090123/146
Use of a Broken or Risky Cryptograp	19-Dec-2022	5.5	A vulnerability, which was classified as problematic, has been found in Click Studios	N/A	A-CLI-PASS-090123/147

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Algorithm			Passwordstate and Passwordstate Browser Extension Chrome. Affected by this issue is some unknown functionality. The manipulation leads to risky cryptographic algorithm. 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-216272. **CVE ID : CVE-2022-4610**		
Use of Hard-coded Credentials	19-Dec-2022	5.3	A vulnerability, which was classified as problematic, was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. This affects an unknown part. The manipulation leads to hard-coded credentials. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The identifier VDB-216273 was assigned to this vulnerability. **CVE ID : CVE-2022-4611**	N/A	A-CLI-PASS-090123/148

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Codeigniter					
Product: codeigniter					
Affected Version(s): From (including) 4.0.0 Up to (excluding) 4.2.11					
Improper Authentication	22-Dec-2022	9.8	CodeIgniter is a PHP full-stack web framework. When an application uses (1) multiple session cookies (e.g., one for user pages and one for admin pages) and (2) a session handler is set to `DatabaseHandler`, `MemcachedHandler`, or `RedisHandler`, then if an attacker gets one session cookie (e.g., one for user pages), they may be able to access pages that require another session cookie (e.g., for admin pages). This issue has been patched, please upgrade to version 4.2.11 or later. As a workaround, use only one session cookie. **CVE ID : CVE-2022-46170**	https://github.com/codeigniter4/CodeIgniter4/commit/f9fb6574fbeb5a4aa63f7ea87296523e10db9328	A-COD-CODE-090123/149
Insufficient Verification of Data Authenticity	22-Dec-2022	7.5	CodeIgniter is a PHP full-stack web framework. This vulnerability may allow attackers to spoof their IP address when the server is behind a reverse proxy. This issue has been patched, please upgrade to version 4.2.11 or later, and configure	https://github.com/codeigniter4/CodeIgniter4/commit/5ca8c99b2db09a2a08a013836628028ddc984659	A-COD-CODE-090123/150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`Config\App::$proxyIPs`. As a workaround, do not use `$request->getIPAddress()`. **CVE ID : CVE-2022-23556**		
Vendor: codelights-shortcodes-and-widgets_project					
Product: codelights-shortcodes-and-widgets					
Affected Version(s): * Up to (including) 1.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2022	4.8	The Sidebar Widgets by CodeLights plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Extra CSS class' parameter in versions up to, and including, 1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2022-4619**	N/A	A-COD-CODE-090123/151
Vendor: collective.contact.widget_project					
Product: collective.contact.widget					
Affected Version(s): * Up to (excluding) 1.12					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2022	6.1	A vulnerability classified as problematic was found in collective.contact.widget up to 1.12. This vulnerability affects the function title of the file src/collective/contact/widget/widgets.py. The manipulation leads to cross site scripting. The attack can be initiated remotely. The name of the patch is 5da36305ca7ed433782be8901c47387406fcda12. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216496. **CVE ID : CVE-2022-4638**	https://github.com/collective/collective.contact.widget/commit/5da36305ca7ed433782be8901c47387406fcda12	A-COL-COLL-090123/152
Vendor: contec					
Product: conprosys_hmi_system					
Affected Version(s): * Up to (including) 3.4.4					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	9.8	CONPROSYS HMI System (CHS) Ver.3.4.4?and earlier allows a remote unauthenticated attacker to execute an arbitrary OS command on the server where the product is running by sending a specially crafted request. **CVE ID : CVE-2022-44456**	https://www.contec.com/download/contract/contract4/?itemid=ea8039aa-3434-4999-9ab6-897aa690210c&downloaditemid=866d7d3c-aae9-438d-87f3-17aa040df90b	A-CON-CONP-090123/153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: covid-19_directory_on_vaccination_system_project					
Product: covid-19_directory_on_vaccination_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2022	6.1	Sourcecodester Covid-19 Directory on Vaccination System 1.0 was discovered to contain a Cross-Site Scripting (XSS) vulnerability via verification.php because the program does not verify the txtvaccinationID parameter. **CVE ID : CVE-2022-46095**	N/A	A-COV-COVI-090123/154
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2022	6.1	A Cross site scripting (XSS) vulnerability in Sourcecodester Online Covid-19 Directory on Vaccination System v1.0 allows attackers to execute arbitrary code via the txtfullname parameter or txtphone parameter to register.php without logging in. **CVE ID : CVE-2022-46096**	N/A	A-COV-COVI-090123/155
Vendor: crmx_project					
Product: crmx					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL	18-Dec-2022	9.8	A vulnerability was found in luckyshot CRMx and classified as critical. This issue affects the function get/save/delete/comment/commentdelete of	https://github.com/luckyshot/CRMx/commit/8c62d274986137d6a1d069	A-CRM-CRMX-090123/156

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			the file index.php. The manipulation leads to sql injection. The attack may be initiated remotely. The name of the patch is 8c62d274986137d6a1d06958a6f75c3553f45f8f. It is recommended to apply a patch to fix this issue. The identifier VDB-216185 was assigned to this vulnerability. **CVE ID : CVE-2022-4592**	58a6f75c3553f45f8f	
Vendor: daloradius					
Product: daloradius					
Affected Version(s): -					
Incorrect Permission Assignment for Critical Resource	21-Dec-2022	5.3	Sensitive Cookie Without 'HttpOnly' Flag in GitHub repository lirantal/daloradius prior to master. **CVE ID : CVE-2022-4630**	https://huntr.dev/bounties/401661ee-40e6-4ee3-a925-3716b96ece5c, https://github.com/lirantal/daloradius/commit/6878619dc661b3009429777a1aeeb383ddc0166b	A-DAL-DALO-090123/157
Vendor: datadoghq					
Product: guarddog					
Affected Version(s): * Up to (excluding) 0.1.5					
Relative Path Traversal	17-Dec-2022	7.8	GuardDog is a CLI tool to identify malicious PyPI packages. Versions prior to 0.1.5 are	https://github.com/DataDog/guarddog/pull/89/	A-DAT-GUAR-090123/158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerable to Relative Path Traversal when scanning a specially-crafted local PyPI package. Running GuardDog against a specially-crafted package can allow an attacker to write an arbitrary file on the machine where GuardDog is executed due to a path traversal vulnerability when extracting the .tar.gz file of the package being scanned, which exists by design in the tarfile.TarFile.extractall function. This issue is patched in version 0.1.5. **CVE ID : CVE-2022-23531**	commits/a56aff58264cb6b7855d71b00dc10c39a5dbd306	
Affected Version(s): * Up to (excluding) 0.1.8					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Dec-2022	6.5	GuardDog is a CLI tool to identify malicious PyPI packages. Versions prior to v0.1.8 are vulnerable to arbitrary file write when scanning a specially-crafted remote PyPI package. Extracting files using shutil.unpack_archive() from a potentially malicious tarball without validating that the destination file path is within the intended destination directory can cause files outside	https://github.com/DataDog/guarddog/commit/37c7d0767ba28f4df46117d478f97652594c491c	A-DAT-GUAR-090123/159

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the destination directory to be overwritten. This issue is patched in version 0.1.8. Potential workarounds include using a safer module, like zipfile, and validating the location of the extracted files and discarding those with malicious paths. **CVE ID : CVE-2022-23530**		
Vendor: deltaww					
Product: dopsoft					
Affected Version(s): *					
Out-of-bounds Read	16-Dec-2022	7.5	Out-of-bounds Read vulnerability in Delta Electronics DOPSoft.This issue affects DOPSoft: All Versions. **CVE ID : CVE-2022-2966**	N/A	A-DEL-DOPS-090123/160
Vendor: devolutions					
Product: remote_desktop_manager					
Affected Version(s): * Up to (excluding) 2022.3.27					
Improper Authentication	21-Dec-2022	8.8	Authentication bypass in local application lock feature in Devolutions Remote Desktop Manager 2022.3.26 and earlier on Windows allows malicious user to access the application. **CVE ID : CVE-2022-4287**	https://devolutions.net/security/advisories/DEVO-2022-0011	A-DEV-REMO-090123/161
Vendor: django-openipam_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: django-openipam					
Affected Version(s): * Up to (excluding) 2022-11-11					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2022	6.1	A vulnerability classified as problematic has been found in django-openipam. This affects an unknown part of the file openipam/report/templates/report/exposed_hosts.html. The manipulation of the argument description leads to cross site scripting. It is possible to initiate the attack remotely. The name of the patch is a6223a1150d60cd036106ba6a8e676c1bfc3cc85. It is recommended to apply a patch to fix this issue. The identifier VDB-216189 was assigned to this vulnerability. **CVE ID : CVE-2022-4595**	https://github.com/openipam/django-openipam/commit/a6223a1150d60cd036106ba6a8e676c1bfc3cc85, https://github.com/openipam/django-openipam/pull/205	A-DJA-DJAN-090123/162
Vendor: django_terms_and_conditions_project					
Product: django_terms_and_conditions					
Affected Version(s): * Up to (excluding) 2.0.11					
URL Redirection to Untrusted Site ('Open Redirect')	17-Dec-2022	6.1	A vulnerability has been found in cyface Terms and Conditions Module up to 2.0.9 and classified as problematic. Affected by this vulnerability is the function returnTo of the file termsandconditions/vi	https://github.com/cyface/django-termsandconditions/pull/239, https://github.com/cyface/django-termsandco	A-DJA-DJAN-090123/163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ews.py. The manipulation leads to open redirect. The attack can be launched remotely. Upgrading to version 2.0.10 is able to address this issue. The name of the patch is 03396a1c2e0af95e12a45c5faef7e47a4b513e1a. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216175. **CVE ID : CVE-2022-4589**	nditions/commit/03396a1c2e0af95e12a45c5faef7e47a4b513e1a	
Vendor: drachtio					
Product: drachtio-server					
Affected Version(s): * Up to (excluding) 0.8.19					
Out-of-bounds Write	18-Dec-2022	7.5	An issue was discovered in the libsofia-sip fork in drachtio-server before 0.8.19. It allows remote attackers to cause a denial of service (daemon crash) via a crafted UDP message that causes a url_canonize2 heap-based buffer over-read because of an off-by-one error. **CVE ID : CVE-2022-47517**	https://github.com/davehorton/sofia-sip/commit/22c1bd191f0acbf11f0c0fbea1845d9bf9dcd47e, https://github.com/davehorton/sofia-sip/commit/bfc79d85c8f3a4798a3305fb98f5a11c11d0d29f	A-DRA-DRAC-090123/164
Affected Version(s): * Up to (excluding) 0.8.20					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	18-Dec-2022	7.5	An issue was discovered in drachtio-server before 0.8.20. It allows remote attackers to cause a denial of service (daemon crash) via a long message in a TCP request that leads to std::length_error. **CVE ID : CVE-2022-47515**	https://github.com/drachtio/drachtio-server/commit/4cf9fe2c420b86c16442215d449d40be777c1911	A-DRA-DRAC-090123/165
Reachable Assertion	18-Dec-2022	7.5	An issue was discovered in the libsofia-sip fork in drachtio-server before 0.8.20. It allows remote attackers to cause a denial of service (daemon crash) via a crafted UDP message that leads to a failure of the libsofia-sip-ua/tport/tport.c self assertion. **CVE ID : CVE-2022-47516**	https://github.com/davehorton/sofia-sip/commit/13b2a135287caa2d67ac6cd5155626821e25b377	A-DRA-DRAC-090123/166
Vendor: easy-static-server_project					
Product: easy-static-server					
Affected Version(s): *					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Dec-2022	7.5	All versions of package easy-static-server are vulnerable to Directory Traversal due to missing input sanitization and sandboxes being employed to the req.url user input that is passed to the server code.	https://security.snyk.io/vuln/SNYK-JS-EASYSTATICSERVER-3153539, https://gist.github.com/lirantal/fdfbe26561788c8194a54bf6d31772c9,	A-EAS-EASY-090123/167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25931	https://github.com/cunjieliu/easyServer/blob/master/index.js%23L27	
Vendor: emby					
Product: emby					
Affected Version(s): 4.6.7.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	In Emby Server 4.6.7.0, the playlist name field is vulnerable to XSS stored where it is possible to steal the administrator access token and flip or steal the media server administrator account. **CVE ID : CVE-2022-36223**	N/A	A-EMB-EMBY-090123/168
Vendor: employee_performance_evaluation_system_project					
Product: employee_performance_evaluation_system					
Affected Version(s): 1.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	4.8	Employee Performance Evaluation System v1.0 was discovered to contain a persistent cross-site scripting (XSS) vulnerability via adding new entries under the Departments and Designations module. **CVE ID : CVE-2022-40435**	N/A	A-EMP-EMPL-090123/169
Vendor: entropymine					
Product: deark					
Affected Version(s): 1.6.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Dec-2022	7.8	Deark v.1.6.2 was discovered to contain a stack overflow via the do_prism_read_palette( ) function at /modules/atari-img.c. **CVE ID : CVE-2022-43289**	N/A	A-ENT-DEAR-090123/170
Vendor: ep-3bookingsystem					
Product: ep-3_bookingsystem					
Affected Version(s): * Up to (excluding) 1.8.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2022	6.1	A vulnerability classified as problematic has been found in ep3-bs up to 1.7.x. This affects an unknown part. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 1.8.0 is able to address this issue. The name of the patch is ef49e709c8adecc3a83cdc6164a67162991d2213. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216495. **CVE ID : CVE-2022-4637**	https://github.com/tkrebs/ep3-bs/issues/564, https://github.com/tkrebs/ep3-bs/commit/ef49e709c8adecc3a83cdc6164a67162991d2213, https://github.com/tkrebs/ep3-bs/releases/tag/1.8.0	A-EP--EP-3-090123/171
Vendor: external_media_project					
Product: external_media					
Affected Version(s): * Up to (excluding) 1.0.36					
Improper Neutralization of	19-Dec-2022	4.8	The External Media WordPress plugin before 1.0.36 does not	N/A	A-EXT-EXTE-090123/172

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2022-3832**		
Vendor: exuberant_ctags_project					
Product: exuberant_ctags					
Affected Version(s): *					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Dec-2022	9.8	A flaw was found in Exuberant Ctags in the way it handles the "-o" option. This option specifies the tag filename. A crafted tag filename specified in the command line or in the configuration file results in arbitrary command execution because the externalSortTags() in sort.c calls the system(3) function in an unsafe way. **CVE ID : CVE-2022-4515**	N/A	A-EXU-EXUB-090123/173
Vendor: F-secure					
Product: safe					
Affected Version(s): * Up to (including) 19.1					
N/A	23-Dec-2022	5.4	F-Secure SAFE Browser 19.1 before 19.2 for	https://www.f-secure.com/	A-F-S-SAFE-090123/174

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android allows an IDN homograph attack. **CVE ID : CVE-2022-47524**	en/home/support/security-advisories/cve-2022-47524	
Vendor: Ffmpeg					
Product: ffmpeg					
Affected Version(s): * Up to (excluding) 5.1					
NULL Pointer Dereference	16-Dec-2022	7.5	An issue was discovered in the FFmpeg package, where vp3_decode_frame in libavcodec/vp3.c lacks check of the return value of av_malloc() and will cause a null pointer dereference, impacting availability. **CVE ID : CVE-2022-3109**	https://bugzilla.redhat.com/show_bug.cgi?id=2153551, https://github.com/FFmpeg/FFmpeg/commit/656cb0450aeb73b25d7d26980af342b37ac4c568	A-FFM-FFMP-090123/175
Vendor: Flatpress					
Product: flatpress					
Affected Version(s): * Up to (including) 1.2.1					
Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')	18-Dec-2022	9.8	PHP Remote File Inclusion in GitHub repository flatpressblog/flatpress prior to 1.3. **CVE ID : CVE-2022-4606**	https://hunt r.dev/bounties/3dab0466-c35d-4163-b3c7-a8666e2f7d95, https://github.com/flatpressblog/flatpress/commit/c30d52b28483e1e512d0d81758d4c149f02b4068	A-FLA-FLAT-090123/176

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3. **CVE ID : CVE-2022-4605**	https://github.com/flatpressblog/flatpress/commit/742f8b04f233e3cc52bed11f79fcc9911faee776, https://hunt r.dev/bounties/df455d44-0dec-470c-b576-8ea86ec5a367	A-FLA-FLAT-090123/177
Vendor: freedom					
Product: securedrop					
Affected Version(s): * Up to (excluding) 2.5.1					
Improper Link Resolution Before File Access ('Link Following')	16-Dec-2022	7.8	A vulnerability was found in Freedom of the Press SecureDrop. It has been rated as critical. Affected by this issue is some unknown functionality of the file gpg-agent.conf. The manipulation leads to symlink following. Local access is required to approach this attack. The name of the patch is b0526a06f8ca713cce74b63e00d3730618d89691. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-215972. **CVE ID : CVE-2022-4563**	https://github.com/freedomofpress/securedrop/commit/b0526a06f8ca713cce74b63e00d3730618d89691	A-FRE-SECU-090123/178
Vendor: Genetechsolutions					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: pie_register					
Affected Version(s): * Up to (excluding) 3.8.1.3					
Cross-Site Request Forgery (CSRF)	19-Dec-2022	6.5	The Registration Forms WordPress plugin before 3.8.1.3 does not have authorisation and CSRF when deleting users via an init action handler, allowing unauthenticated attackers to delete arbitrary users (along with their posts) **CVE ID : CVE-2022-4024**	N/A	A-GEN-PIE_-090123/179
Vendor: ghinstallation_project					
Product: ghinstallation					
Affected Version(s): * Up to (excluding) 2.0.0					
Generation of Error Message Containing Sensitive Information	20-Dec-2022	4.7	ghinstallation provides transport, which implements http.RoundTripper to provide authentication as an installation for GitHub Apps. In ghinstallation version 1, when the request to refresh an installation token failed, the HTTP request and response would be returned for debugging. The request contained the bearer JWT for the App, and was returned back to clients. This token is short lived (10 minute maximum). This issue has been patched and is available in version 2.0.0.	https://github.com/bradleyfalzon/ghinstallation/security/advisories/GHSA-h4q8-96p6-jcgr, https://github.com/bradleyfalzon/ghinstallation/commit/d24f14f8be70d94129d76026e8b0f4f9170c8c3e	A-GHI-GHIN-090123/180

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-39304		
Vendor: ghost					
Product: ghost					
Affected Version(s): 5.9.4					
Observable Response Discrepancy	22-Dec-2022	5.3	A user enumeration vulnerability exists in the login functionality of Ghost Foundation Ghost 5.9.4. A specially-crafted HTTP request can lead to a disclosure of sensitive information. An attacker can send a series of HTTP requests to trigger this vulnerability. **CVE ID : CVE-2022-41697**	N/A	A-GHO-GHOS-090123/181
Affected Version(s): From (including) 4.46.0 Up to (excluding) 4.48.8					
Improper Access Control	22-Dec-2022	4.3	An authentication bypass vulnerability exists in the newsletter subscription functionality of Ghost Foundation Ghost 5.9.4. A specially-crafted HTTP request can lead to increased privileges. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-41654**	https://github.com/TryGhost/Ghost/security/advisories/GHSA-9gh8-wp53-ccc6	A-GHO-GHOS-090123/182
Affected Version(s): From (including) 5.0.0 Up to (excluding) 5.22.7					
Improper Access Control	22-Dec-2022	4.3	An authentication bypass vulnerability exists in the newsletter subscription functionality of Ghost	https://github.com/TryGhost/Ghost/security/advisories/GH	A-GHO-GHOS-090123/183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Foundation Ghost 5.9.4. A specially-crafted HTTP request can lead to increased privileges. An attacker can send an HTTP request to trigger this vulnerability. **CVE ID : CVE-2022-41654**	SA-9gh8-wp53-ccc6	
Vendor: GNU					
Product: grub2					
Affected Version(s): * Up to (including) 2.06					
Out-of-bounds Write	19-Dec-2022	7.1	When rendering certain unicode sequences, grub2's font code doesn't proper validate if the informed glyph's width and height is constrained within bitmap size. As consequence an attacker can craft an input which will lead to a out-of-bounds write into grub2's heap, leading to memory corruption and availability issues. Although complex, arbitrary code execution could not be discarded. **CVE ID : CVE-2022-3775**	N/A	A-GNU-GRUB-090123/184
Vendor: grafana					
Product: enterprise_metrics					
Affected Version(s): From (including) 1.0.0 Up to (excluding) 1.7.1					
N/A	20-Dec-2022	8.8	A vulnerability in the label-based access control of Grafana Labs Grafana Enterprise	https://grafana.com/docs/enterprise-	A-GRA-ENTE-090123/185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Metrics allows an attacker more access than intended. If an access policy which has label selector restrictions also has been granted access to all tenants in the system, the label selector restrictions will not be applied when using this policy with the affected versions of the software. This issue affects: Grafana Labs Grafana Enterprise Metrics GEM 1.X versions prior to 1.7.1 on AMD64; GEM 2.X versions prior to 2.3.1 on AMD64. **CVE ID : CVE-2022-44643**	metrics/v2.4.x/downloads/#v171----november-14th-2022, https://grafana.com/docs/enterprise-metrics/v2.4.x/downloads/#v231----november-14th-2022	
Affected Version(s): From (including) 2.0.0 Up to (excluding) 2.3.1					
N/A	20-Dec-2022	8.8	A vulnerability in the label-based access control of Grafana Labs Grafana Enterprise Metrics allows an attacker more access than intended. If an access policy which has label selector restrictions also has been granted access to all tenants in the system, the label selector restrictions will not be applied when using this policy with the affected versions of the	https://grafana.com/docs/enterprise-metrics/v2.4.x/downloads/#v171----november-14th-2022, https://grafana.com/docs/enterprise-metrics/v2.4.x/downloads/#v231----november-14th-2022	A-GRA-ENTE-090123/186

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			software. This issue affects: Grafana Labs Grafana Enterprise Metrics GEM 1.X versions prior to 1.7.1 on AMD64; GEM 2.X versions prior to 2.3.1 on AMD64. **CVE ID : CVE-2022-44643**		
Vendor: hcltech					
Product: bigfix_platform					
Affected Version(s): From (including) 10 Up to (including) 10.0.7					
Inadequate Encryption Strength	19-Dec-2022	7.8	In specific scenarios, on Windows the operator credentials may be encrypted in a manner that is not completely machine-dependent. **CVE ID : CVE-2022-38659**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0102049	A-HCL-BIGF-090123/187
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.8					
Improper Authentication	19-Dec-2022	6.5	There are insufficient warnings when a Fixlet is imported by a user. The warning message currently assumes the owner of the script is the logged in user, with insufficient warnings when attempting to run the script. **CVE ID : CVE-2022-42453**	N/A	A-HCL-BIGF-090123/188
Affected Version(s): From (including) 9.5 Up to (including) 9.5.20					
Inadequate Encryption Strength	19-Dec-2022	7.8	In specific scenarios, on Windows the operator credentials may be encrypted in a manner	https://support.hcltechsw.com/csm?id=kb_article&sysparm_a	A-HCL-BIGF-090123/189

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			that is not completely machine-dependent. **CVE ID : CVE-2022-38659**	rticle=KB0102049	
Affected Version(s): From (including) 9.5.0 Up to (excluding) 9.5.21					
Improper Authentication	19-Dec-2022	6.5	There are insufficient warnings when a Fixlet is imported by a user. The warning message currently assumes the owner of the script is the logged in user, with insufficient warnings when attempting to run the script. **CVE ID : CVE-2022-42453**	N/A	A-HCL-BIGF-090123/190
Product: bigfix_server_automation					
Affected Version(s): * Up to (including) 3.2.1					
N/A	24-Dec-2022	7.5	BigFix deployments that have installed the Notification Service on Windows are susceptible to disclosing SMTP BigFix operator's sensitive data in clear text. Operators who use Notification Service related content from BES Support are at risk of leaving their SMTP sensitive data exposed. **CVE ID : CVE-2022-38658**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0102117	A-HCL-BIGF-090123/191
Product: bigfix_webui					
Affected Version(s): 20					
N/A	21-Dec-2022	5.8	BigFix WebUI non-master operators are missing controls that	https://support.hcltechsw.com/csm?	A-HCL-BIGF-090123/192

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prevent them from being able to modify the relevance of fixlets or to deploy fixlets from the BES Support external site. **CVE ID : CVE-2022-38655**	id=kb_article&sysparm_article=KB0102140	
Product: digital_experience					
Affected Version(s): 9.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	In HCL Digital Experience, customized XSS payload can be constructed such that it is served in the application unencoded. **CVE ID : CVE-2022-38653**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0102141	A-HCL-DIGI-090123/193
Affected Version(s): 8.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	In HCL Digital Experience, customized XSS payload can be constructed such that it is served in the application unencoded. **CVE ID : CVE-2022-38653**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0102141	A-HCL-DIGI-090123/194
Affected Version(s): 9.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	In HCL Digital Experience, customized XSS payload can be constructed such that it is served in the application unencoded. **CVE ID : CVE-2022-38653**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0102141	A-HCL-DIGI-090123/195
Product: hcl_digital_experience					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 9.5					
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2022	6.1	In HCL Digital Experience, URLs can be constructed to redirect users to untrusted sites. **CVE ID : CVE-2022-38662**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0102141	A-HCL-HCL_-090123/196
Affected Version(s): 8.5					
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2022	6.1	In HCL Digital Experience, URLs can be constructed to redirect users to untrusted sites. **CVE ID : CVE-2022-38662**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0102141	A-HCL-HCL_-090123/197
Affected Version(s): 9.0					
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2022	6.1	In HCL Digital Experience, URLs can be constructed to redirect users to untrusted sites. **CVE ID : CVE-2022-38662**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0102141	A-HCL-HCL_-090123/198
Vendor: hcltechsw					
Product: bigfix_insights_for_vulnerability_remediation					
Affected Version(s): * Up to (including) 2.0					
Improper Input Validation	21-Dec-2022	6.5	Insights for Vulnerability Remediation (IVR) is vulnerable to improper input validation. This may lead to information disclosure. This requires privileged access. **CVE ID : CVE-2022-44756**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0102168	A-HCL-BIGF-090123/199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	21-Dec-2022	5.3	Insights for Vulnerability Remediation (IVR) is vulnerable to man-in-the-middle attacks that may lead to information disclosure. This requires privileged network access. **CVE ID : CVE-2022-42454**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0102168	A-HCL-BIGF-090123/200
Vendor: hutool					
Product: hutool					
Affected Version(s): * Up to (including) 5.8.10					
Improper Resource Shutdown or Release	16-Dec-2022	7.5	A vulnerability classified as problematic was found in Dromara HuTool up to 5.8.10. This vulnerability affects unknown code of the file cn.hutool.core.util.ZipUtil.java. The manipulation leads to resource consumption. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 5.8.11 is able to address this issue. It is recommended to upgrade the affected component. VDB-215974 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4565**	N/A	A-HUT-HUTO-090123/201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: IBM					
Product: cognos_analytics					
Affected Version(s): 11.1.7					
Server-Side Request Forgery (SSRF)	19-Dec-2022	9.1	IBM Cognos Analytics 11.1.7 11.2.0, and 11.2.1 could be vulnerable to a Server-Side Request Forgery Attack (SSRF) attack by constructing URLs from user-controlled data. This could enable attackers to make arbitrary requests to the internal network or to the local file system. IBM X-Force ID: 234180. **CVE ID : CVE-2022-38708**	https://www.ibm.com/support/pages/node/6841801, https://exchange.xforce.ibmcloud.com/vulnerabilities/234180	A-IBM-COGN-090123/202
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Dec-2022	7.5	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could be vulnerable to a Log Injection attack by constructing URLs from user-controlled data. This could enable attackers to make arbitrary requests to the internal network or to the local file system. IBM X-Force ID: 240266. **CVE ID : CVE-2022-43883**	https://www.ibm.com/support/pages/node/6841801, https://exchange.xforce.ibmcloud.com/vulnerabilities/240266	A-IBM-COGN-090123/203
Improper Neutralization of Input During Web Page	19-Dec-2022	6.1	IBM Cognos Analytics 11.2.1, 11.2.0, and 11.1.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed	https://www.ibm.com/support/pages/node/6841801, https://exch	A-IBM-COGN-090123/204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			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: 235064. **CVE ID : CVE-2022-39160**	ange.xforce.ibmcloud.com/vulnerabilities/235064	
Insertion of Sensitive Information into Log File	19-Dec-2022	5.3	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could be vulnerable to sensitive information exposure by passing API keys to log files. If these keys contain sensitive information, it could lead to further attacks. IBM X-Force ID: 240450. **CVE ID : CVE-2022-43887**	https://www.ibm.com/support/pages/node/6841801, https://exchange.xforce.ibmcloud.com/vulnerabilities/240450	A-IBM-COGN-090123/205
Affected Version(s): From (including) 11.1.0 Up to (excluding) 11.1.7					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	6.1	IBM Cognos Analytics 11.2.1, 11.2.0, and 11.1.7 is vulnerable to 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: 235064. **CVE ID : CVE-2022-39160**	https://www.ibm.com/support/pages/node/6841801, https://exchange.xforce.ibmcloud.com/vulnerabilities/235064	A-IBM-COGN-090123/206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Insertion of Sensitive Information into Log File	19-Dec-2022	5.3	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could be vulnerable to sensitive information exposure by passing API keys to log files. If these keys contain sensitive information, it could lead to further attacks. IBM X-Force ID: 240450. **CVE ID : CVE-2022-43887**	https://www.ibm.com/support/pages/node/6841801, https://exchange.xforce.ibmcloud.com/vulnerabilities/240450	A-IBM-COGN-090123/207
Affected Version(s): From (including) 11.1.0 Up to (including) 11.1.7					
Server-Side Request Forgery (SSRF)	19-Dec-2022	9.1	IBM Cognos Analytics 11.1.7 11.2.0, and 11.2.1 could be vulnerable to a Server-Side Request Forgery Attack (SSRF) attack by constructing URLs from user-controlled data. This could enable attackers to make arbitrary requests to the internal network or to the local file system. IBM X-Force ID: 234180. **CVE ID : CVE-2022-38708**	https://www.ibm.com/support/pages/node/6841801, https://exchange.xforce.ibmcloud.com/vulnerabilities/234180	A-IBM-COGN-090123/208
Improper Neutralization of Special Elements in Output Used by a Downstream Componen	19-Dec-2022	7.5	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could be vulnerable to a Log Injection attack by constructing URLs from user-controlled data. This could enable attackers to make arbitrary requests to	https://www.ibm.com/support/pages/node/6841801, https://exchange.xforce.ibmcloud.com/vulnerabi	A-IBM-COGN-090123/209

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
t ('Injection')			the internal network or to the local file system. IBM X-Force ID: 240266. **CVE ID : CVE-2022-43883**	lities/240266	
Affected Version(s): From (including) 11.2.0 Up to (including) 11.2.3					
Server-Side Request Forgery (SSRF)	19-Dec-2022	9.1	IBM Cognos Analytics 11.1.7 11.2.0, and 11.2.1 could be vulnerable to a Server-Side Request Forgery Attack (SSRF) attack by constructing URLs from user-controlled data. This could enable attackers to make arbitrary requests to the internal network or to the local file system. IBM X-Force ID: 234180. **CVE ID : CVE-2022-38708**	https://www.ibm.com/support/pages/node/6841801, https://exchange.xforce.ibmcloud.com/vulnerabilities/234180	A-IBM-COGN-090123/210
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Dec-2022	7.5	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could be vulnerable to a Log Injection attack by constructing URLs from user-controlled data. This could enable attackers to make arbitrary requests to the internal network or to the local file system. IBM X-Force ID: 240266. **CVE ID : CVE-2022-43883**	https://www.ibm.com/support/pages/node/6841801, https://exchange.xforce.ibmcloud.com/vulnerabilities/240266	A-IBM-COGN-090123/211

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	6.1	IBM Cognos Analytics 11.2.1, 11.2.0, and 11.1.7 is vulnerable to 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: 235064. **CVE ID : CVE-2022-39160**	https://www.ibm.com/support/pages/node/6841801, https://exchange.xforce.ibmcloud.com/vulnerabilities/235064	A-IBM-COGN-090123/212
Insertion of Sensitive Information into Log File	19-Dec-2022	5.3	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could be vulnerable to sensitive information exposure by passing API keys to log files. If these keys contain sensitive information, it could lead to further attacks. IBM X-Force ID: 240450. **CVE ID : CVE-2022-43887**	https://www.ibm.com/support/pages/node/6841801, https://exchange.xforce.ibmcloud.com/vulnerabilities/240450	A-IBM-COGN-090123/213
Product: domino					
Affected Version(s): * Up to (excluding) 9.0.1.10					
Out-of-bounds Write	19-Dec-2022	7.8	IBM Domino is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute	N/A	A-IBM-DOMI-090123/214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44754. **CVE ID : CVE-2022-44750**		
Out-of-bounds Write	19-Dec-2022	7.8	IBM Domino is susceptible to a stack based buffer overflow vulnerability in wp6sr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted WordPerfect file. **CVE ID : CVE-2022-44752**	N/A	A-IBM-DOMI-090123/215
Out-of-bounds Write	19-Dec-2022	7.8	IBM Domino is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44750. **CVE ID : CVE-2022-44754**	N/A	A-IBM-DOMI-090123/216
Affected Version(s): 9.0.1.10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	19-Dec-2022	7.8	IBM Domino is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44754. **CVE ID : CVE-2022-44750**	N/A	A-IBM-DOMI-090123/217
Out-of-bounds Write	19-Dec-2022	7.8	IBM Domino is susceptible to a stack based buffer overflow vulnerability in wp6sr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted WordPerfect file. **CVE ID : CVE-2022-44752**	N/A	A-IBM-DOMI-090123/218
Out-of-bounds Write	19-Dec-2022	7.8	IBM Domino is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute	N/A	A-IBM-DOMI-090123/219

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44750. **CVE ID : CVE-2022-44754**		
Product: financial_transaction_manager					
Affected Version(s): 3.2.4					
Improper Input Validation	20-Dec-2022	5.5	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 could allow an authenticated user to lock additional RM authorizations, resulting in a denial of service on displaying or managing these authorizations. IBM X-Force ID: 240034. **CVE ID : CVE-2022-43875**	https://www.ibm.com/support/pages/node/6848881, https://exchange.xforce.ibmcloud.com/vulnerabilities/240034	A-IBM-FINA-090123/220
Incorrect Authorization	20-Dec-2022	5.3	IBM Financial Transaction Manager 3.2.4 authorization checks are done incorrectly for some HTTP requests which allows getting unauthorized technical information (e.g. event log entries) about the FTM SWIFT system. IBM X-Force ID: 239708. **CVE ID : CVE-2022-43872**	https://www.ibm.com/support/pages/node/6848881, https://exchange.xforce.ibmcloud.com/vulnerabilities/239708	A-IBM-FINA-090123/221
Product: notes					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 9.0.1.10					
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44755. **CVE ID : CVE-2022-44751**	N/A	A-IBM-NOTE-090123/222
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow vulnerability in wp6sr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted WordPerfect file. **CVE ID : CVE-2022-44753**	N/A	A-IBM-NOTE-090123/223
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated	N/A	A-IBM-NOTE-090123/224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44751. **CVE ID : CVE-2022-44755**		
Affected Version(s): 9.0.1.10					
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44755. **CVE ID : CVE-2022-44751**	N/A	A-IBM-NOTE-090123/225
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow vulnerability in wp6sr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted WordPerfect file.	N/A	A-IBM-NOTE-090123/226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44753		
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44751. **CVE ID : CVE-2022-44755**	N/A	A-IBM-NOTE-090123/227
Affected Version(s): 10.0.1					
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44755. **CVE ID : CVE-2022-44751**	N/A	A-IBM-NOTE-090123/228
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow	N/A	A-IBM-NOTE-090123/229

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability in wp6sr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted WordPerfect file. **CVE ID : CVE-2022-44753**		
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44751. **CVE ID : CVE-2022-44755**	N/A	A-IBM-NOTE-090123/230
Affected Version(s): From (including) 10.0.0 Up to (excluding) 10.0.1					
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a	N/A	A-IBM-NOTE-090123/231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44755. **CVE ID : CVE-2022-44751**		
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow vulnerability in wp6sr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted WordPerfect file. **CVE ID : CVE-2022-44753**	N/A	A-IBM-NOTE-090123/232
Out-of-bounds Write	19-Dec-2022	7.8	IBM Notes is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44751. **CVE ID : CVE-2022-44755**	N/A	A-IBM-NOTE-090123/233
Product: security_guardium					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 11.4					
N/A	20-Dec-2022	4.9	IBM Security Guardium 11.4 could allow a privileged user to obtain sensitive information inside of an HTTP response. IBM X-Force ID: 235405. **CVE ID : CVE-2022-39166**	https://www.ibm.com/support/pages/node/6848317, https://exchange.xforce.ibmcloud.com/vulnerabilities/235405	A-IBM-SECU-090123/234
Product: security_verify_governance					
Affected Version(s): 10.0.1					
Use of a Broken or Risky Cryptographic Algorithm	22-Dec-2022	7.5	IBM Security Verify Governance, Identity Manager 10.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 225007. **CVE ID : CVE-2022-22461**	https://www.ibm.com/support/pages/node/6850845, https://exchange.xforce.ibmcloud.com/vulnerabilities/225077	A-IBM-SECU-090123/235
Insufficiently Protected Credentials	22-Dec-2022	6.5	IBM Security Verify Governance, Identity Manager 10.0.1 stores user credentials in plain clear text which can be read by a remote authenticated user. IBM X-Force ID: 225009. **CVE ID : CVE-2022-22458**	https://exchange.xforce.ibmcloud.com/vulnerabilities/225009, https://www.ibm.com/support/pages/node/6849247	A-IBM-SECU-090123/236
Improper Neutralization of Input During	22-Dec-2022	6.1	IBM Security Verify Governance, Identity Manager 10.0.1 is vulnerable to cross-site scripting. This	https://exchange.xforce.ibmcloud.com/vulnerabilities/22500	A-IBM-SECU-090123/237

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			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: 225004. **CVE ID : CVE-2022-22456**	4, https://www.ibm.com/support/pages/node/6849247	
Generation of Error Message Containing Sensitive Information	24-Dec-2022	5.3	IBM Security Verify Governance, Identity Manager 10.01 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 224915. **CVE ID : CVE-2022-22449**	https://exchange.xforce.ibmcloud.com/vulnerabilities/224915, https://www.ibm.com/support/pages/node/6849247	A-IBM-SECU-090123/238
Improper Authentication	22-Dec-2022	5.3	IBM Security Verify Governance, Identity Manager 10.0.1 software component could allow an authenticated user to modify or cancel any other user's access request using man-in-the-middle techniques. IBM X-Force ID: 231096. **CVE ID : CVE-2022-35646**	https://exchange.xforce.ibmcloud.com/vulnerabilities/231096, https://www.ibm.com/support/pages/node/6850809	A-IBM-SECU-090123/239

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	22-Dec-2022	4.4	IBM Security Verify Governance, Identity Manager 10.0.1 stores sensitive information including user credentials in plain clear text which can be read by a local privileged user. IBM X-Force ID: 225007. **CVE ID : CVE-2022-22457**	https://exchange.xforce.ibmcloud.com/vulnerabilities/225007, https://www.ibm.com/support/pages/node/6849247	A-IBM-SECU-090123/240
Product: spectrum_control					
Affected Version(s): 5.4.0.0					
Use of a Broken or Risky Cryptographic Algorithm	20-Dec-2022	7.5	IBM Spectrum Control 5.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 233982. **CVE ID : CVE-2022-38391**	https://www.ibm.com/support/pages/node/6847541, https://exchange.xforce.ibmcloud.com/vulnerabilities/233982	A-IBM-SPEC-090123/241
Product: spectrum_scale					
Affected Version(s): * Up to (including) 5.1.4.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Dec-2022	6.8	IBM Spectrum Scale 5.1 could allow users with permissions to create pod, persistent volume and persistent volume claim to access files and directories outside of the volume, including on the host filesystem. IBM X-Force ID: 235740. **CVE ID : CVE-2022-40607**	https://exchange.xforce.ibmcloud.com/vulnerabilities/235740, https://www.ibm.com/support/pages/node/6848231	A-IBM-SPEC-090123/242
Product: urbancode_deploy					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 7.3.0.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2022	4.6	IBM UrbanCode Deploy (UCD) 6.2.0.0 through 6.2.7.18, 7.0.5.0 through 7.0.5.13, 7.1.0.0 through 7.1.2.9, 7.2.0.0 through 7.2.3.2 and 7.3.0.0 is vulnerable to 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: 242273. **CVE ID : CVE-2022-46771**	https://exchange.xforce.ibmcloud.com/vulnerabilities/242273, https://www.ibm.com/support/pages/node/6848897	A-IBM-URBA-090123/243
Affected Version(s): From (including) 6.2.0.0 Up to (including) 6.2.7.18					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2022	4.6	IBM UrbanCode Deploy (UCD) 6.2.0.0 through 6.2.7.18, 7.0.5.0 through 7.0.5.13, 7.1.0.0 through 7.1.2.9, 7.2.0.0 through 7.2.3.2 and 7.3.0.0 is vulnerable to 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: 242273. **CVE ID : CVE-2022-46771**	https://exchange.xforce.ibmcloud.com/vulnerabilities/242273, https://www.ibm.com/support/pages/node/6848897	A-IBM-URBA-090123/244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 7.0.5.0 Up to (including) 7.0.5.13					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2022	4.6	IBM UrbanCode Deploy (UCD) 6.2.0.0 through 6.2.7.18, 7.0.5.0 through 7.0.5.13, 7.1.0.0 through 7.1.2.9, 7.2.0.0 through 7.2.3.2 and 7.3.0.0 is vulnerable to 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: 242273. **CVE ID : CVE-2022-46771**	https://exchange.xforce.ibmcloud.com/vulnerabilities/242273, https://www.ibm.com/support/pages/node/6848897	A-IBM-URBA-090123/245
Affected Version(s): From (including) 7.1.0.0 Up to (including) 7.1.2.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2022	4.6	IBM UrbanCode Deploy (UCD) 6.2.0.0 through 6.2.7.18, 7.0.5.0 through 7.0.5.13, 7.1.0.0 through 7.1.2.9, 7.2.0.0 through 7.2.3.2 and 7.3.0.0 is vulnerable to 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: 242273. **CVE ID : CVE-2022-46771**	https://exchange.xforce.ibmcloud.com/vulnerabilities/242273, https://www.ibm.com/support/pages/node/6848897	A-IBM-URBA-090123/246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 7.2.0.0 Up to (including) 7.2.3.2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Dec-2022	4.6	IBM UrbanCode Deploy (UCD) 6.2.0.0 through 6.2.7.18, 7.0.5.0 through 7.0.5.13, 7.1.0.0 through 7.1.2.9, 7.2.0.0 through 7.2.3.2 and 7.3.0.0 is vulnerable to 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: 242273. **CVE ID : CVE-2022-46771**	https://exchange.xforce.ibmcloud.com/vulnerabilities/242273, https://www.ibm.com/support/pages/node/6848897	A-IBM-URBA-090123/247
Product: vios					
Affected Version(s): 3.1					
Improper Privilege Management	23-Dec-2022	8.4	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the rm_rlcache_file command to obtain root privileges. IBM X-Force ID: 236690. **CVE ID : CVE-2022-41290**	https://www.ibm.com/support/pages/node/6847917, https://exchange.xforce.ibmcloud.com/vulnerabilities/236690	A-IBM-VIOS-090123/248
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to cause a denial	https://www.ibm.com/support/pages/node/6847947	A-IBM-VIOS-090123/249

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of service. IBM X-Force ID: 235181. **CVE ID : CVE-2022-39164**		
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in CAA to cause a denial of service. IBM X-Force ID: 235183. **CVE ID : CVE-2022-39165**	https://exchange.xforce.ibmcloud.com/vulnerabilities/235183, https://www.ibm.com/support/pages/node/6847947	A-IBM-VIOS-090123/250
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 235599. **CVE ID : CVE-2022-40233**	https://exchange.xforce.ibmcloud.com/vulnerabilities/235599, https://www.ibm.com/support/pages/node/6847947	A-IBM-VIOS-090123/251
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX NFS kernel extension to cause a denial of service. IBM X-Force ID: 238640. **CVE ID : CVE-2022-43380**	https://www.ibm.com/support/pages/node/6847947, https://exchange.xforce.ibmcloud.com/vulnerabilities/238640	A-IBM-VIOS-090123/252
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX	https://www.ibm.com/support/pages/node/6851443,	A-IBM-VIOS-090123/253

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			SMB client to cause a denial of service. IBM X-Force ID: 238639. **CVE ID : CVE-2022-43381**	https://exchange.xforce.ibmcloud.com/vulnerabilities/238639	
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX perfstat kernel extension to cause a denial of service. IBM X-Force ID: 239169. **CVE ID : CVE-2022-43848**	https://www.ibm.com/support/pages/node/6847947, https://exchange.xforce.ibmcloud.com/vulnerabilities/239169	A-IBM-VIOS-090123/254
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX pfcdd kernel extension to cause a denial of service. IBM X-Force ID: 239170. **CVE ID : CVE-2022-43849**	https://exchange.xforce.ibmcloud.com/vulnerabilities/239170, https://www.ibm.com/support/pages/node/6847947	A-IBM-VIOS-090123/255
N/A	20-Dec-2022	4.4	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a local user with elevated privileges to exploit a vulnerability in the lpd daemon to cause a denial of service. IBM X-Force ID: 238641. **CVE ID : CVE-2022-43382**	https://www.ibm.com/support/pages/node/6848309, https://exchange.xforce.ibmcloud.com/vulnerabilities/238641	A-IBM-VIOS-090123/256
Vendor: ikus-soft					
Product: rdiffweb					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.5.4					
Cross-Site Request Forgery (CSRF)	22-Dec-2022	6.5	Cross-Site Request Forgery (CSRF) in GitHub repository ikus060/rdiffweb prior to 2.5.4. **CVE ID : CVE-2022-4646**	https://hunt r.dev/bounti es/17bc1b0f -1f5c-432f-88e4-c9866ccf6e1 0, https://gith ub.com/ikus 060/rdiffwe b/commit/e 6f0d800212 9be90fe82fa 3e3ea0a694 2caba398	A-IKU-RDIF-090123/257
URL Redirectio n to Untrusted Site ('Open Redirect')	22-Dec-2022	6.1	Open Redirect in GitHub repository ikus060/rdiffweb prior to 2.5.4. **CVE ID : CVE-2022-4644**	https://gith ub.com/ikus 060/rdiffwe b/commit/5 f861670ef8f 38ca8eea52 a98672d0e0 fabb5368, https://hunt r.dev/bounti es/77e5f425 -c764-4cb0-936a-7a76bfcf19b 0	A-IKU-RDIF-090123/258
Vendor: inex					
Product: ixp_manager					
Affected Version(s): * Up to (excluding) 6.3.0					
Improper Neutralizat ion of Input During Web Page Generation	16-Dec-2022	6.1	A vulnerability was found in INEX IPX-Manager up to 6.2.0. It has been declared as problematic. This vulnerability affects unknown code of the file	https://gith ub.com/inex /IXP-Manager/co mmit/bc9b1 4c6f70cccdb 89b559e8bc	A-INE-IXP_-090123/259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			resources/views/customer/list.foil.php. The manipulation leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 6.3.0 is able to address this issue. The name of the patch is bc9b14c6f70cccdb89b559e8bc3a7318bfe9c243. It is recommended to upgrade the affected component. VDB-215962 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4559**	3a7318bfe9c243	
Vendor: inhabit					
Product: move_crm					
Affected Version(s): 4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2022	5.4	Inhabit Systems Pty Ltd Move CRM version 4, build 260 was discovered to contain a cross-site scripting (XSS) vulnerability via the User profile component. **CVE ID : CVE-2022-43271**	https://inhabit.com.au/CVE-2022-43271	A-INH-MOVE-090123/260
Vendor: iofinnet					
Product: tss-lib					
Affected Version(s): * Up to (excluding) 2.0.0					
Use of a Broken or Risky Cryptograp	23-Dec-2022	9.1	IO FinNet tss-lib before 2.0.0 allows a collision of hash values. **CVE ID : CVE-2022-47931**	https://github.com/IoFinnet/tss-lib/commit/369ec50be1437588a973	A-IOF-TSS--090123/261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
hic Algorithm				3443bcb2f15b794601d4	
Vendor: Isode					
Product: m-vault					
Affected Version(s): From (including) 16.0v0 Up to (including) 17.0v3					
N/A	21-Dec-2022	7.5	Isode M-Vault 16.0v0 through 17.x before 17.0v24 can crash upon an LDAP v1 bind request. **CVE ID : CVE-2022-47581**	https://www.isode.com/support/security/advisory/m-vault-denial-of-service-21-12-2022.html	A-ISO-M-VA-090123/262
Vendor: jacic					
Product: electronic_bidding_core_system					
Affected Version(s): * Up to (excluding) 6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	6.1	Cross-site scripting vulnerability in DENSHI NYUSATSU CORE SYSTEM v6 R4 and earlier allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2022-41993**	https://www.cals.jacic.or.jp/coreconso/pdf/coreconsoinfo20221215.pdf	A-JAC-ELEC-090123/263
Affected Version(s): * Up to (including) 6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	6.1	Cross-site scripting vulnerability in DENSHI NYUSATSU CORE SYSTEM v6 R4 and earlier allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2022-46287**	https://www.cals.jacic.or.jp/coreconso/pdf/coreconsoinfo20221215.pdf	A-JAC-ELEC-090123/264

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2022	6.1	Open redirect vulnerability in DENSHI NYUSATSU CORE SYSTEM v6 R4 and earlier allows a remote unauthenticated attacker to redirect a user to an arbitrary web site and conduct a phishing attack by having a user to access a specially crafted URL. **CVE ID : CVE-2022-46288**	https://www.cals.jacic.or.jp/coreconso/pdf/coreconsoinfo20221215.pdf	A-JAC-ELEC-090123/265
Affected Version(s): 6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	6.1	Cross-site scripting vulnerability in DENSHI NYUSATSU CORE SYSTEM v6 R4 and earlier allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2022-41993**	https://www.cals.jacic.or.jp/coreconso/pdf/coreconsoinfo20221215.pdf	A-JAC-ELEC-090123/266
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	6.1	Cross-site scripting vulnerability in DENSHI NYUSATSU CORE SYSTEM v6 R4 and earlier allows a remote unauthenticated attacker to inject an arbitrary script. **CVE ID : CVE-2022-46287**	https://www.cals.jacic.or.jp/coreconso/pdf/coreconsoinfo20221215.pdf	A-JAC-ELEC-090123/267
URL Redirection to Untrusted Site ('Open Redirect')	19-Dec-2022	6.1	Open redirect vulnerability in DENSHI NYUSATSU CORE SYSTEM v6 R4 and earlier allows a remote unauthenticated attacker to redirect a	https://www.cals.jacic.or.jp/coreconso/pdf/coreconsoinfo20221215.pdf	A-JAC-ELEC-090123/268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user to an arbitrary web site and conduct a phishing attack by having a user to access a specially crafted URL. **CVE ID : CVE-2022-46288**		
Vendor: jegtheme					
Product: jeg_elementor_kit					
Affected Version(s): * Up to (excluding) 2.5.7					
Authorization Bypass Through User-Controlled Key	22-Dec-2022	7.5	The Jeg Elementor Kit plugin for WordPress is vulnerable to authorization bypass in various functions used to update the plugin settings in versions up to, and including, 2.5.6. Unauthenticated users can use an easily available nonce, obtained from pages edited by the plugin, to update the MailChimp API key, global styles, 404 page settings, and enabled elements. **CVE ID : CVE-2022-3805**	N/A	A-JEG-JEG_-090123/269
Authorization Bypass Through User-Controlled Key	22-Dec-2022	4.3	The Jeg Elementor Kit plugin for WordPress is vulnerable to authorization bypass in various AJAX actions in versions up to, and including, 2.5.6. Authenticated users can use an easily available nonce value to create header templates and make additional changes to the site, as	N/A	A-JEG-JEG_-090123/270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the plugin does not use capability checks for this purpose. **CVE ID : CVE-2022-3794**		
Vendor: Jetbrains					
Product: intellij_idea					
Affected Version(s): * Up to (excluding) 2022.3.1					
Improper Control of Generation of Code ('Code Injection')	22-Dec-2022	7.8	In JetBrains IntelliJ IDEA before 2022.3.1 code Templates were vulnerable to SSTI attacks. **CVE ID : CVE-2022-47896**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-090123/271
Cleartext Transmission of Sensitive Information	22-Dec-2022	7.5	In JetBrains IntelliJ IDEA before 2022.3.1 the "Validate JSP File" action used the HTTP protocol to download required JAR files. **CVE ID : CVE-2022-47895**	https://www.jetbrains.com/privacy-security/issues-fixed/	A-JET-INTE-090123/272
Vendor: joget					
Product: joget_dx					
Affected Version(s): * Up to (including) 7.0.32					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	A vulnerability was found in Joget up to 7.0.31. It has been rated as problematic. This issue affects the function getInternalJsCssLib of the file wflow-core/src/main/java/org/joget/plugin/enterprise/UniversalTheme.java of the component wflow-core. The manipulation of the	https://github.com/jogetworkflow/jw-community/commit/ecf8be8f6f0cb725c18536ddc726d42a11bdaa1b	A-JOG-JOGE-090123/273

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			argument key leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 7.0.32 is able to address this issue. The name of the patch is ecf8be8f6f0cb725c18536ddc726d42a11bdaa1b. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-215963. **CVE ID : CVE-2022-4560**		
Vendor: json5					
Product: json5					
Affected Version(s): * Up to (excluding) 2.2.2					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	24-Dec-2022	8.8	JSON5 is an extension to the popular JSON file format that aims to be easier to write and maintain by hand (e.g. for config files). The `parse` method of the JSON5 library before and including version `2.2.1` does not restrict parsing of keys named `__proto__`, allowing specially crafted strings to pollute the prototype of the resulting object. This vulnerability pollutes the prototype of the object returned by `JSON5.parse` and not the global Object prototype, which is the commonly understood	https://github.com/json5/json5/issues/199	A-JSO-JSON-090123/274

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			definition of Prototype Pollution. However, polluting the prototype of a single object can have significant security impact for an application if the object is later used in trusted operations. This vulnerability could allow an attacker to set arbitrary and unexpected keys on the object returned from `JSON5.parse`. The actual impact will depend on how applications utilize the returned object and how they filter unwanted keys, but could include denial of service, cross-site scripting, elevation of privilege, and in extreme cases, remote code execution. `JSON5.parse` should restrict parsing of `__proto__` keys when parsing JSON strings to objects. As a point of reference, the `JSON.parse` method included in JavaScript ignores `__proto__` keys. Simply changing `JSON5.parse` to `JSON.parse` in the examples above mitigates this vulnerability. This vulnerability is patched		

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in json5 version 2.2.2 and later. **CVE ID : CVE-2022-46175**		
Vendor: Linuxfoundation					
Product: cortex					
Affected Version(s): 1.13.0					
N/A	19-Dec-2022	6.5	Cortex provides multi-tenant, long term storage for Prometheus. A local file inclusion vulnerability exists in Cortex versions 1.13.0, 1.13.1 and 1.14.0, where a malicious actor could remotely read local files as a result of parsing maliciously crafted Alertmanager configurations when submitted to the Alertmanager Set Configuration API. Only users of the Alertmanager service where `-experimental.alertmanager.enable-api` or `enable_api: true` is configured are affected. Affected Cortex users are advised to upgrade to patched versions 1.13.2 or 1.14.1. However as a workaround, Cortex administrators may reject Alertmanager configurations containing the `api_key_file` setting in the `opsgenie_configs`	https://cortexmetrics.io/docs/api/#set-alertmanager-configuration	A-LIN-CORT-090123/275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			section before sending to the Set Alertmanager Configuration API. **CVE ID : CVE-2022-23536**		
Affected Version(s): 1.13.1					
N/A	19-Dec-2022	6.5	Cortex provides multi-tenant, long term storage for Prometheus. A local file inclusion vulnerability exists in Cortex versions 1.13.0, 1.13.1 and 1.14.0, where a malicious actor could remotely read local files as a result of parsing maliciously crafted Alertmanager configurations when submitted to the Alertmanager Set Configuration API. Only users of the Alertmanager service where `-experimental.alertmanager.enable-api` or `enable_api: true` is configured are affected. Affected Cortex users are advised to upgrade to patched versions 1.13.2 or 1.14.1. However as a workaround, Cortex administrators may reject Alertmanager configurations containing the `api_key_file` setting in the `opsgenie_configs` section before sending	https://cortexmetrics.io/docs/api/#set-alertmanager-configuration	A-LIN-CORT-090123/276

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to the Set Alertmanager Configuration API. **CVE ID : CVE-2022-23536**		
Affected Version(s): 1.14.0					
N/A	19-Dec-2022	6.5	Cortex provides multi-tenant, long term storage for Prometheus. A local file inclusion vulnerability exists in Cortex versions 1.13.0, 1.13.1 and 1.14.0, where a malicious actor could remotely read local files as a result of parsing maliciously crafted Alertmanager configurations when submitted to the Alertmanager Set Configuration API. Only users of the Alertmanager service where `-experimental.alertmanager.enable-api` or `enable_api: true` is configured are affected. Affected Cortex users are advised to upgrade to patched versions 1.13.2 or 1.14.1. However as a workaround, Cortex administrators may reject Alertmanager configurations containing the `api_key_file` setting in the `opsgenie_configs` section before sending to the Set Alertmanager Configuration API.	https://cortexmetrics.io/docs/api/#set-alertmanager-configuration	A-LIN-CORT-090123/277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-23536		
Vendor: liquidjs					
Product: liquidjs					
Affected Version(s): * Up to (excluding) 10.0.0					
Exposure of Sensitive Information to an Unauthorized Actor	22-Dec-2022	5.3	The package liquidjs before 10.0.0 are vulnerable to Information Exposure when ownPropertyOnly parameter is set to False, which results in leaking properties of a prototype. Workaround For versions 9.34.0 and higher, an option to disable this functionality is provided. **CVE ID : CVE-2022-25948**	https://github.com/harttle/liquidjs/commit/7e99efc5131e20cf3f59e1fc2c371a15aa4109db, https://security.snyk.io/vuln/SNYK-JS-LIQUIDJS-2952868, https://github.com/harttle/liquidjs/issues/454	A-LIQ-LIQU-090123/278
Vendor: lite-server_project					
Product: lite-server					
Affected Version(s): -					
N/A	20-Dec-2022	7.5	All versions of package lite-server are vulnerable to Denial of Service (DoS) when an attacker sends an HTTP request and includes control characters that the decodeURI() function is unable to parse. **CVE ID : CVE-2022-25940**	https://security.snyk.io/vuln/SNYK-JS-LITESERVER-3153540, https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-3175617, https://gist.github.com/lirantal/8323	A-LIT-LITE-090123/279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				82155e00da92bfd8bb3adea474eb	
Vendor: Mediawiki					
Product: semantic_drilldown					
Affected Version(s): * Up to (excluding) 2022-08-12					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	A vulnerability classified as problematic has been found in SemanticDrilldown Extension. Affected is the function printFilterLine of the file includes/specials/SDBrowseDataPage.php of the component GET Parameter Handler. The manipulation of the argument value leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is 6e18cf740a4548166c1d95f6d3a28541d298a3aa. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-215964. **CVE ID : CVE-2022-4561**	https://github.com/wikimedia/mediawiki-extensions-SemanticDrilldown/commit/6e18cf740a4548166c1d95f6d3a28541d298a3aa	A-MED-SEMA-090123/280
Vendor: Microfocus					
Product: groupwise					
Affected Version(s): * Up to (excluding) 18.4.2					
Insertion of Sensitive Informatio	16-Dec-2022	4.3	A vulnerability has been identified in Micro Focus GroupWise Web in versions prior to	https://portal.microfocus.com/s/article/KM0000	A-MIC-GROU-090123/281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n into Log File			18.4.2. The GW Web component makes a request to the Post Office Agent that contains sensitive information in the query parameters that could be logged by any intervening HTTP proxies. **CVE ID : CVE-2022-38756**	12374?language=en_US	
Vendor: Microweber					
Product: microweber					
Affected Version(s): * Up to (including) 1.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2022	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.3.2. **CVE ID : CVE-2022-4617**	https://hunt r.dev/bounties/1fb2ce08-7016-45fa-b402-ec08d700e4df, https://github.com/microweber/microweber/commit/df8add930ecfa7f5b18c67c3f748c137fe890906	A-MIC-MICR-090123/282
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2022	6.1	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.3.2. **CVE ID : CVE-2022-4647**	https://github.com/microweber/microweber/commit/20df56615e61624f5fff149849753869e4b3b936, https://hunt r.dev/bounti	A-MIC-MICR-090123/283

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				es/ccdd243d-726c-4199-b742-25c571491242	
Vendor: mind-map_project					
Product: mind-map					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-2022	6.1	A vulnerability was found in 1j01 mind-map and classified as problematic. This issue affects some unknown processing of the file app.coffee. The manipulation of the argument html leads to cross site scripting. The attack may be initiated remotely. The name of the patch is 9617e6084dfeccd92079ab4d7f439300a4b24394. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216167. **CVE ID : CVE-2022-4581**	https://github.com/1j01/mind-map/commit/9617e6084dfeccd92079ab4d7f439300a4b24394	A-MIN-MIND-090123/284
Vendor: mingsoft					
Product: mcms					
Affected Version(s): 5.2.9					
Improper Neutralization of Input During Web Page Generation	21-Dec-2022	5.4	A vulnerability has been found in Mingsoft MCMS 5.2.9 and classified as problematic. Affected by this vulnerability is the function save of the	N/A	A-MIN-MCMS-090123/285

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			component Article Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216499. **CVE ID : CVE-2022-4640**		
Vendor: Misp-project					
Product: malware_information_sharing_platform					
Affected Version(s): * Up to (excluding) 2.4.167					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2022	6.1	In MISP before 2.4.167, there is XSS in the template file uploads in app/View/Templates/upload_file.ctp. **CVE ID : CVE-2022-47928**	https://github.com/MISP/MISP/commit/684d3e51398d4ea032b06fa4a1cd2bdf7d8b0ede	A-MIS-MALW-090123/286
Vendor: Mozilla					
Product: firefox					
Affected Version(s): * Up to (excluding) 100.0					
Reachable Assertion	22-Dec-2022	9.8	Mozilla developers Andrew McCreight, Gabriele Svelto, Tom Ritter and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 99 and Firefox ESR 91.8. Some of these bugs	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1684739%2C1706441%2C1753298%2C1762614%2C1762620	A-MOZ-FIRE-090123/287

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100. **CVE ID : CVE-2022-29917**	%2C1764778, https://www.mozilla.org/security/advisories/mfsa2022-17/, https://www.mozilla.org/security/advisories/mfsa2022-16/	
Incorrect Default Permissions	22-Dec-2022	8.8	Documents in deeply-nested cross-origin browsing contexts could have obtained permissions granted to the top-level origin, bypassing the existing prompt and wrongfully inheriting the top-level permissions. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100. **CVE ID : CVE-2022-29909**	https://www.mozilla.org/security/advisories/mfsa2022-17/, https://www.mozilla.org/security/advisories/mfsa2022-16/, https://bugzilla.mozilla.org/show_bug.cgi?id=1755081	A-MOZ-FIRE-090123/288
N/A	22-Dec-2022	6.5	Firefox behaved slightly differently for already known resources when loading CSS resources involving CSS variables. This could have been used to probe the browser history. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.	https://bugzilla.mozilla.org/show_bug.cgi?id=1760674, https://www.mozilla.org/security/advisories/mfsa2022-17/, https://www.mozilla.org/security/advisories/mf	A-MOZ-FIRE-090123/289

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-29916	sa2022-16/, https://www.mozilla.org/security/advisories/mfsa2022-18/	
URL Redirection to Untrusted Site ('Open Redirect')	22-Dec-2022	6.1	When closed or sent to the background, Firefox for Android would not properly record and persist HSTS settings. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 100. **CVE ID : CVE-2022-29910**	https://bugzilla.mozilla.org/show_bug.cgi?id=1757138, https://www.mozilla.org/security/advisories/mfsa2022-16/	A-MOZ-FIRE-090123/290
Affected Version(s): * Up to (excluding) 100.0.2					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	22-Dec-2022	8.8	An attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1. **CVE ID : CVE-2022-1529**	https://bugzilla.mozilla.org/show_bug.cgi?id=1770048, https://www.mozilla.org/security/advisories/mfsa2022-19/	A-MOZ-FIRE-090123/291

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	22-Dec-2022	8.8	If an attacker was able to corrupt the methods of an Array object in JavaScript via prototype pollution, they could have achieved execution of attacker-controlled JavaScript code in a privileged context. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1. **CVE ID : CVE-2022-1802**	https://bugzilla.mozilla.org/show_bug.cgi?id=1770137, https://www.mozilla.org/security/advisories/mfsa2022-19/	A-MOZ-FIRE-090123/292
Affected Version(s): * Up to (excluding) 100.3.0					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	22-Dec-2022	8.8	An attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1. **CVE ID : CVE-2022-1529**	https://bugzilla.mozilla.org/show_bug.cgi?id=1770048, https://www.mozilla.org/security/advisories/mfsa2022-19/	A-MOZ-FIRE-090123/293
Improperly Controlled Modificatio	22-Dec-2022	8.8	If an attacker was able to corrupt the methods of an Array object in	https://bugzilla.mozilla.org/show_bu	A-MOZ-FIRE-090123/294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
n of Object Prototype Attributes ('Prototype Pollution')			JavaScript via prototype pollution, they could have achieved execution of attacker-controlled JavaScript code in a privileged context. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1. **CVE ID : CVE-2022-1802**	g.cgi?id=1770137, https://www.mozilla.org/security/advisories/mfsa2022-19/	
Affected Version(s): * Up to (excluding) 101					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2022	9.8	The search term could have been specified externally to trigger SQL injection. This vulnerability affects Firefox for iOS < 101. **CVE ID : CVE-2022-1887**	https://bugzilla.mozilla.org/show_bug.cgi?id=1767205, https://www.mozilla.org/security/advisories/mfsa2022-23/	A-MOZ-FIRE-090123/295
Affected Version(s): * Up to (excluding) 102.0					
N/A	22-Dec-2022	8.8	An iframe that was not permitted to run scripts could do so if the user clicked on a <code>javascript:</code> link. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34468**	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://bugzilla.mozilla.org/show_bug.cgi?id=1768537, https://www.mozilla.org/security/advisories/mfsa2022-26/,	A-MOZ-FIRE-090123/296

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://www.mozilla.org/security/advisories/mfsa2022-25/	
Access of Uninitialized Pointer	22-Dec-2022	8.8	Within the <code>lg_init()</code> function, if several allocations succeed but then one fails, an uninitialized pointer would have been freed despite never being allocated. This vulnerability affects Firefox < 102. **CVE ID : CVE-2022-34480**	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://bugzilla.mozilla.org/show_bug.cgi?id=1454072	A-MOZ-FIRE-090123/297
Integer Overflow or Wraparound	22-Dec-2022	8.8	In the <code>nsTArray_Impl::ReplaceElementsAt()</code> function, an integer overflow could have occurred when the number of elements to replace was too large for the container. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34481**	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://bugzilla.mozilla.org/show_bug.cgi?id=1497246, https://www.mozilla.org/security/advisories/mfsa2022-26/, https://www.mozilla.org/security/advisories/mfsa2022-25/	A-MOZ-FIRE-090123/298
N/A	22-Dec-2022	8.8	An attacker who could have convinced a user to drag and drop an image to a filesystem could have manipulated	https://www.mozilla.org/security/advisories/mfsa2022-24/,	A-MOZ-FIRE-090123/299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the resulting filename to contain an executable extension, and by extension potentially tricked the user into executing malicious code. While very similar, this is a separate issue from CVE-2022-34483. This vulnerability affects Firefox < 102. **CVE ID : CVE-2022-34482**	https://bugzilla.mozilla.org/show_bug.cgi?id=845880	
N/A	22-Dec-2022	8.8	An attacker who could have convinced a user to drag and drop an image to a filesystem could have manipulated the resulting filename to contain an executable extension, and by extension potentially tricked the user into executing malicious code. While very similar, this is a separate issue from CVE-2022-34482. This vulnerability affects Firefox < 102. **CVE ID : CVE-2022-34483**	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://bugzilla.mozilla.org/show_bug.cgi?id=1335845	A-MOZ-FIRE-090123/300
Reachable Assertion	22-Dec-2022	8.8	The Mozilla Fuzzing Team reported potential vulnerabilities present in Thunderbird 91.10. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1763634%2C1	A-MOZ-FIRE-090123/301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have been exploited to run arbitrary code. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34484**	772651, https://www.mozilla.org/security/advisories/mfsa2022-26/, https://www.mozilla.org/security/advisories/mfsa2022-25/	
N/A	22-Dec-2022	6.5	A malicious website that could create a popup could have resized the popup to overlay the address bar with its own content, resulting in potential user confusion or spoofing attacks. *This bug only affects Thunderbird for Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34479**	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://www.mozilla.org/security/advisories/mfsa2022-26/, https://www.mozilla.org/security/advisories/mfsa2022-25/, https://bugzilla.mozilla.org/show_bug.cgi?id=1745595	A-MOZ-FIRE-090123/302
Affected Version(s): * Up to (excluding) 104.0					
Out-of-bounds Write	22-Dec-2022	8.8	Members the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 103, Firefox ESR 102.1, and Firefox ESR 91.12. Some of these bugs showed evidence of memory corruption and we presume that with	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1770630%2C1776658, https://www.mozilla.org/security/advisories/mf	A-MOZ-FIRE-090123/303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 102.2, Thunderbird < 91.13, Firefox ESR < 91.13, Firefox ESR < 102.2, and Firefox < 104. **CVE ID : CVE-2022-38478**	sa2022-35/, https://www.mozilla.org/security/advisories/mfsa2022-34/, https://www.mozilla.org/security/advisories/mfsa2022-33/	
Affected Version(s): * Up to (excluding) 105.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2022	6.1	When injecting an HTML base element, some requests would ignore the CSP's base-uri settings and accept the injected element's base instead. This vulnerability affects Firefox ESR < 102.3, Thunderbird < 102.3, and Firefox < 105. **CVE ID : CVE-2022-40956**	https://www.mozilla.org/security/advisories/mfsa2022-42/, https://www.mozilla.org/security/advisories/mfsa2022-41/, https://www.mozilla.org/security/advisories/mfsa2022-40/, https://bugzilla.mozilla.org/show_bug.cgi?id=1770094	A-MOZ-FIRE-090123/304
Out-of-bounds Read	22-Dec-2022	5.5	An out-of-bounds read can occur when decoding H264 video. This results in a potentially exploitable crash. This vulnerability affects Firefox ESR < 102.3, Thunderbird <	https://www.mozilla.org/security/advisories/mfsa2022-42/, https://www.mozilla.org/security/advisories/mfsa2022-41/,	A-MOZ-FIRE-090123/305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			102.3, and Firefox < 105. **CVE ID : CVE-2022-3266**	https://www.mozilla.org/security/advisories/mfsa2022-40/, https://bugzilla.mozilla.org/show_bug.cgi?id=1767360	
Affected Version(s): * Up to (excluding) 106.0					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Dec-2022	7.1	If two Workers were simultaneously initializing their CacheStorage, a data race could have occurred in the <code>ThirdPartyUtil</ /code> component. This vulnerability affects Firefox < 106. **CVE ID : CVE-2022-42930**	https://www.mozilla.org/security/advisories/mfsa2022-44/, https://bugzilla.mozilla.org/show_bug.cgi?id=1789503	A-MOZ-FIRE-090123/306
Affected Version(s): * Up to (excluding) 107.0					
N/A	22-Dec-2022	7.8	When downloading an HTML file, if the title of the page was formatted as a filename with a malicious extension, Firefox may have saved the file with that extension, leading to possible system compromise if the downloaded file was later ran. This vulnerability affects Firefox < 107. **CVE ID : CVE-2022-45415**	https://www.mozilla.org/security/advisories/mfsa2022-47/, https://bugzilla.mozilla.org/show_bug.cgi?id=1793551	A-MOZ-FIRE-090123/307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	22-Dec-2022	6.1	Using the <code>S.browser_fallback_url parameter</code> parameter, an attacker could redirect a user to a URL and cause SameSite=Strict cookies to be sent. *This issue only affects Firefox for Android. Other operating systems are not affected.*. This vulnerability affects Firefox < 107. **CVE ID : CVE-2022-45413**	https://bugzilla.mozilla.org/show_bug.cgi?id=1791201, https://www.mozilla.org/security/advisories/mfsa2022-47/	A-MOZ-FIRE-090123/308
Affected Version(s): * Up to (excluding) 96.0					
Out-of-bounds Write	22-Dec-2022	8.8	Applying a CSS filter effect could have accessed out of bounds memory. This could have lead to a heap-buffer-overflow causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22738**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/, https://bugzilla.mozilla.org/show_bug.cgi?id=1742382	A-MOZ-FIRE-090123/309
Use After Free	22-Dec-2022	8.8	Certain network request objects were freed too early when releasing a network	https://www.mozilla.org/security/advisories/mf	A-MOZ-FIRE-090123/310

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request handle. This could have lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22740**	sa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1742334, https://www.mozilla.org/security/advisories/mfsa2022-03/	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Dec-2022	8.8	The constructed curl command from the "Copy as curl" feature in DevTools was not properly escaped for PowerShell. This could have lead to command injection if pasted into a Powershell prompt. *This bug only affects Thunderbird for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22744**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/311
Out-of-bounds Write	22-Dec-2022	8.8	Mozilla developers Calixte Denizet, Kershaw Chang, Christian Holler, Jason Kratzer, Gabriele Svelto, Tyson Smith, Simon	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://ww	A-MOZ-FIRE-090123/312

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Giesecke, and Steve Fink reported memory safety bugs present in Firefox 95 and Firefox ESR 91.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22751**	w.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	
Out-of-bounds Write	22-Dec-2022	8.8	Mozilla developers Christian Holler and Jason Kratzer reported memory safety bugs present in Firefox 95. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 96. **CVE ID : CVE-2022-22752**	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1741210%2C1742770, https://www.mozilla.org/security/advisories/mfsa2022-01/	A-MOZ-FIRE-090123/313
N/A	22-Dec-2022	8.8	When a worker is shutdown, it was possible to cause script to run late in the lifecycle, at a point after where it should not be possible. This vulnerability affects	https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/a	A-MOZ-FIRE-090123/314

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 96, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22763**	dvisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://bugzilla.mozilla.org/show_bug.cgi?id=1740534	
Use After Free	22-Dec-2022	7.5	Constructing audio sinks could have lead to a race condition when playing audio files and closing windows. This could have lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22737**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1745874, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/315
N/A	22-Dec-2022	7.5	When resizing a popup while requesting fullscreen access, the popup would have become unable to leave fullscreen mode. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://ww	A-MOZ-FIRE-090123/316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22741	w.mozilla.org/security/advisories/mfsa2022-03/	
N/A	22-Dec-2022	7	If Firefox was installed to a world-writable directory, a local privilege escalation could occur when Firefox searched the current directory for system libraries. However the install directory is not world-writable by default. *This bug only affects Firefox for Windows in a non-default installation. Other operating systems are unaffected.*. This vulnerability affects Firefox < 96. **CVE ID : CVE-2022-22736**	https://bugzilla.mozilla.org/show_bug.cgi?id=1742692, https://www.mozilla.org/security/advisories/mfsa2022-01/	A-MOZ-FIRE-090123/317
N/A	22-Dec-2022	6.5	Malicious websites could have tricked users into accepting launching a program to handle an external URL protocol. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22739**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1744158, https://www.mozilla.or	A-MOZ-FIRE-090123/318

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				g/security/advisories/mfsa2022-03/	
Out-of-bounds Read	22-Dec-2022	6.5	When inserting text while in edit mode, some characters might have lead to out-of-bounds memory access causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22742**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/319
N/A	22-Dec-2022	6.5	Securitypolicyviolation events could have leaked cross-origin information for frame-ancestors violations. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22745**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/320
Improper Certificate Validation	22-Dec-2022	6.5	After accepting an untrusted certificate, handling an empty pkcs7 sequence as part of the certificate data could have lead to a crash. This crash is believed to be unexploitable. This vulnerability affects	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/,	A-MOZ-FIRE-090123/321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22747**	https://bugzilla.mozilla.org/show_bug.cgi?id=1735028, https://www.mozilla.org/security/advisories/mfsa2022-03/	
N/A	22-Dec-2022	6.5	Malicious websites could have confused Firefox into showing the wrong origin when asking to launch a program and handling an external URL protocol. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22748**	https://bugzilla.mozilla.org/show_bug.cgi?id=1705211, https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/322
N/A	22-Dec-2022	6.5	By generally accepting and passing resource handles across processes, a compromised content process might have confused higher privileged processes to interact with handles that the unprivileged process should not have access to. *This bug only affects Firefox for	https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1566608	A-MOZ-FIRE-090123/323

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Windows and MacOS. Other operating systems are unaffected.*. This vulnerability affects Firefox < 96. **CVE ID : CVE-2022-22750**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Dec-2022	5.9	A race condition could have allowed bypassing the fullscreen notification which could have lead to a fullscreen window spoof being unnoticed. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22746**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/324
N/A	22-Dec-2022	4.3	When navigating from inside an iframe while requesting fullscreen access, an attacker-controlled tab could have made the browser unable to leave fullscreen mode. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22743**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/325
N/A	22-Dec-2022	4.3	When scanning QR codes, Firefox for	https://www.mozilla.or	A-MOZ-FIRE-090123/326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android would have allowed navigation to some URLs that do not point to web content. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 96. **CVE ID : CVE-2022-22749**	g/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1705094	
Affected Version(s): * Up to (excluding) 97.0					
N/A	22-Dec-2022	9.6	If a document created a sandboxed iframe without <code>allow-scripts</code>, and subsequently appended an element to the iframe's document that e.g. had a JavaScript event handler - the event handler would have run despite the iframe's sandbox. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22759**	https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/, https://bugzilla.mozilla.org/show_bug.cgi?id=1739957	A-MOZ-FIRE-090123/327
Out-of-bounds Write	22-Dec-2022	8.8	Mozilla developers and community members Gabriele Svelto, Sebastian Hengst, Randell Jesup, Luan Herrera, Lars T Hansen, and the Mozilla Fuzzing Team reported memory safety bugs present in	https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/328

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox 96. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 97. **CVE ID : CVE-2022-0511**		
Out-of-bounds Write	22-Dec-2022	8.8	Mozilla developers Kershaw Chang, Ryan VanderMeulen, and Randell Jesup reported memory safety bugs present in Firefox 97. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 98. **CVE ID : CVE-2022-0843**	https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1746523%2C1749062%2C1749164%2C1749214%2C1749610%2C1750032%2C1752100%2C1752405%2C1753612%2C1754508	A-MOZ-FIRE-090123/329
Operation on a Resource after Expiration or Release	22-Dec-2022	8.8	By using XSL Transforms, a malicious webserver could have served a user an XSL document that would continue to execute JavaScript (within the bounds of the same-origin policy) even after the tab was closed. This	https://bugzilla.mozilla.org/show_bug.cgi?id=1309630, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/330

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox < 97. **CVE ID : CVE-2022-22755**		
N/A	22-Dec-2022	8.8	If a user was convinced to drag and drop an image to their desktop or other folder, the resulting object could have been changed into an executable script which would have run arbitrary code after the user clicked on it. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22756**	https://bugzilla.mozilla.org/show_bug.cgi?id=1317873, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/331
Cleartext Transmission of Sensitive Information	22-Dec-2022	8.8	When clicking on a tel: link, USSD codes, specified after a <code>*</code> character, would be included in the phone number. On certain phones, or on certain carriers, if the number was dialed this could perform actions on a user's account, similar to a cross-site request forgery attack. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This	https://bugzilla.mozilla.org/show_bug.cgi?id=1728742, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox < 97. **CVE ID : CVE-2022-22758**		
N/A	22-Dec-2022	8.8	Web-accessible extension pages (pages with a moz-extension:// scheme) were not correctly enforcing the frame-ancestors directive when it was used in the Web Extension's Content Security Policy. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22761**	https://bugzilla.mozilla.org/show_bug.cgi?id=1745566, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/333
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Dec-2022	8.8	Mozilla developers Paul Adenot and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 96 and Firefox ESR 91.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6.	https://www.mozilla.org/security/advisories/mfsa2022-06/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1742682%2C1744165%2C1746545%2C1748210%2C1748279, https://www.mozilla.org/security/advisories/mfsa2022-05/	A-MOZ-FIRE-090123/334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22764		
Time-of-check Time-of-use (TOCTOU) Race Condition	22-Dec-2022	7.1	A Time-of-Check Time-of-Use bug existed in the Maintenance (Updater) Service that could be abused to grant Users write access to an arbitrary directory. This could have been used to escalate to SYSTEM access. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22753**	https://bugzilla.mozilla.org/show_bug.cgi?id=1732435, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/335
Incorrect Authorization	22-Dec-2022	6.5	If a user installed an extension of a particular type, the extension could have auto-updated itself and while doing so, bypass the prompt which grants the new version the new requested permissions. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22754**	https://www.mozilla.org/security/advisories/mfsa2022-06/, https://bugzilla.mozilla.org/show_bug.cgi?id=1750565, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/336

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	22-Dec-2022	6.5	Remote Agent, used in WebDriver, did not validate the Host or Origin headers. This could have allowed websites to connect back locally to the user's browser to control it. *This bug only affected Firefox when WebDriver was enabled, which is not the default configuration.*. This vulnerability affects Firefox < 97. **CVE ID : CVE-2022-22757**	https://bugzilla.mozilla.org/show_bug.cgi?id=1720098, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/337
Generation of Error Message Containing Sensitive Information	22-Dec-2022	6.5	When importing resources using Web Workers, error messages would distinguish the difference between <code>application/javascript</code> responses and non-script responses. This could have been abused to learn information cross-origin. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22760**	https://bugzilla.mozilla.org/show_bug.cgi?id=1748503, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/338
N/A	22-Dec-2022	4.3	Under certain circumstances, a JavaScript alert (or prompt) could have	https://bugzilla.mozilla.org/show_bug.cgi?id=174	A-MOZ-FIRE-090123/339

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			been shown while another website was displayed underneath it. This could have been abused to trick the user. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 97. **CVE ID : CVE-2022-22762**	3931, https://www.mozilla.org/security/advisories/mfsa2022-04/	
Affected Version(s): * Up to (excluding) 97.0.2					
Use After Free	22-Dec-2022	9.6	An unexpected message in the WebGPU IPC framework could lead to a use-after-free and exploitable sandbox escape. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0. **CVE ID : CVE-2022-26486**	https://bugzilla.mozilla.org/show_bug.cgi?id=1758070, https://www.mozilla.org/security/advisories/mfsa2022-09/	A-MOZ-FIRE-090123/340
Use After Free	22-Dec-2022	8.8	Removing an XSLT parameter during processing could have lead to an exploitable use-after-free. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1,	https://bugzilla.mozilla.org/show_bug.cgi?id=1758062, https://www.mozilla.org/security/advisories/mfsa2022-09/	A-MOZ-FIRE-090123/341

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0. **CVE ID : CVE-2022-26485**		
Affected Version(s): * Up to (excluding) 97.3.0					
Use After Free	22-Dec-2022	9.6	An unexpected message in the WebGPU IPC framework could lead to a use-after-free and exploitable sandbox escape. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0. **CVE ID : CVE-2022-26486**	https://bugzilla.mozilla.org/show_bug.cgi?id=1758070, https://www.mozilla.org/security/advisories/mfsa2022-09/	A-MOZ-FIRE-090123/342
Use After Free	22-Dec-2022	8.8	Removing an XSLT parameter during processing could have lead to an exploitable use-after-free. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0. **CVE ID : CVE-2022-26485**	https://bugzilla.mozilla.org/show_bug.cgi?id=1758062, https://www.mozilla.org/security/advisories/mfsa2022-09/	A-MOZ-FIRE-090123/343
Affected Version(s): * Up to (excluding) 98.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Dec-2022	9.6	If an attacker could control the contents of an iframe sandboxed with <code>allow-popups</code> but not <code>allow-scripts</code>, they were able to craft a link that, when clicked, would lead to JavaScript execution in violation of the sandbox. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7. **CVE ID : CVE-2022-26384**	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/, https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1744352	A-MOZ-FIRE-090123/344
Use After Free	22-Dec-2022	8.8	An attacker could have caused a use-after-free by forcing a text reflow in an SVG object leading to a potentially exploitable crash. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7. **CVE ID : CVE-2022-26381**	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/, https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1736243	A-MOZ-FIRE-090123/345
Time-of-check Time-of-	22-Dec-2022	7.5	When installing an add-on, Firefox verified the signature before	https://www.mozilla.org/security/a	A-MOZ-FIRE-090123/346

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
use (TOCTOU) Race Condition			prompting the user; but while the user was confirming the prompt, the underlying add-on file could have been modified and Firefox would not have noticed. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7. **CVE ID : CVE-2022-26387**	dvisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/, https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1752979	
Use After Free	22-Dec-2022	6.5	In unusual circumstances, an individual thread may outlive the thread's manager during shutdown. This could have led to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox < 98. **CVE ID : CVE-2022-26385**	https://bugzilla.mozilla.org/show_bug.cgi?id=1747526, https://www.mozilla.org/security/advisories/mfsa2022-10/	A-MOZ-FIRE-090123/347
Observable Discrepancy	22-Dec-2022	4.3	While the text displayed in Autofill tooltips cannot be directly read by JavaScript, the text was rendered using page fonts. Side-channel attacks on the text by using specially crafted fonts could have lead to this text being inferred by the webpage. This	https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1741888	A-MOZ-FIRE-090123/348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox < 98. **CVE ID : CVE-2022-26382**		
N/A	22-Dec-2022	4.3	When resizing a popup after requesting fullscreen access, the popup would not display the fullscreen notification. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7. **CVE ID : CVE-2022-26383**	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/, https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1742421	A-MOZ-FIRE-090123/349
Affected Version(s): * Up to (excluding) 99.0					
Out-of-bounds Write	22-Dec-2022	8.8	If a compromised content process sent an unexpected number of WebAuthN Extensions in a Register command to the parent process, an out of bounds write would have occurred leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28281**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1755621, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/a	A-MOZ-FIRE-090123/350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				dvisories/mfsa2022-14/	
N/A	22-Dec-2022	8.8	SVG's <code><use></code> element could have been used to load unexpected content that could have executed script in certain circumstances. While the specification seems to allow this, other browsers do not, and web developers relied on this property for script security so gecko's implementation was aligned with theirs. This vulnerability affects Firefox < 99. **CVE ID : CVE-2022-28284**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1754522	A-MOZ-FIRE-090123/351
Out-of-bounds Write	22-Dec-2022	8.8	Mozilla developers and community members Randell Jesup, Sebastian Hengst, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 98. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 99. **CVE ID : CVE-2022-28288**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1746415%2C1746495%2C1746500%2C1747282%2C1748759%2C1749056%2C1749786%2C1751679%2C1752120%2C1756010%2C1756017%2C	A-MOZ-FIRE-090123/352

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				1757213%2C1757258%2C1757427	
Out-of-bounds Write	22-Dec-2022	8.8	Mozilla developers and community members Nika Layzell, Andrew McCreight, Gabriele Svelto, and the Mozilla Fuzzing Team reported memory safety bugs present in Thunderbird 91.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28289**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1663508%2C1744525%2C1753508%2C1757476%2C1757805%2C1758549%2C1758776, https://www.mozilla.org/security/advisories/mfsa2022-15/	A-MOZ-FIRE-090123/353
Use After Free	22-Dec-2022	6.5	<code>NSSToken</code> objects were referenced via direct points, and could have been accessed in an unsafe way on different threads, leading to a use-after-free and potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-1097**	https://bugzilla.mozilla.org/show_bug.cgi?id=1745667, https://www.mozilla.org/security/advisories/mfsa2022-13/, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/a	A-MOZ-FIRE-090123/354

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				dvisories/mfsa2022-14/	
Use After Free	22-Dec-2022	6.5	By using a link with <code>rel="localization "</code> a use-after-free could have been triggered by destroying an object during JavaScript execution and then referencing the object through a freed pointer, leading to a potential exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28282**	https://bugzilla.mozilla.org/show_bug.cgi?id=1751609, https://www.mozilla.org/security/advisories/mfsa2022-13/, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/advisories/mfsa2022-14/	A-MOZ-FIRE-090123/355
N/A	22-Dec-2022	6.5	The sourceMapURL feature in devtools was missing security checks that would have allowed a webpage to attempt to include local files or other files that should have been inaccessible. This vulnerability affects Firefox < 99. **CVE ID : CVE-2022-28283**	https://bugzilla.mozilla.org/show_bug.cgi?id=1754066, https://www.mozilla.org/security/advisories/mfsa2022-13/	A-MOZ-FIRE-090123/356
N/A	22-Dec-2022	6.5	When generating the assembly code for <code>MLoadTypedArrayElementHole</code>, an incorrect AliasSet was used. In conjunction with another vulnerability	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://www.mozilla.org/security/a	A-MOZ-FIRE-090123/357

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this could have been used for an out of bounds memory read. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28285**	dvisories/mfsa2022-15/, https://bugzilla.mozilla.org/show_bug.cgi?id=1756957, https://www.mozilla.org/security/advisories/mfsa2022-14/	
N/A	22-Dec-2022	6.5	In unusual circumstances, selecting text could cause text selection caching to behave incorrectly, leading to a crash. This vulnerability affects Firefox < 99. **CVE ID : CVE-2022-28287**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1741515	A-MOZ-FIRE-090123/358
Improper Restriction of Rendered UI Layers or Frames	22-Dec-2022	5.4	Due to a layout change, iframe contents could have been rendered outside of its border. This could have led to user confusion or spoofing attacks. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28286**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1735265, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/advisories/mfsa2022-14/	A-MOZ-FIRE-090123/359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 101.0					
Out-of-bounds Write	22-Dec-2022	9.8	Mozilla developers Bryce Seager van Dyk and the Mozilla Fuzzing Team reported potential vulnerabilities present in Firefox 101. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 102. **CVE ID : CVE-2022-34485**	https://www.mozilla.org/security/advisories/mfsa2022-24/	A-MOZ-FIRE-090123/360
Affected Version(s): 101.0.1					
Out-of-bounds Write	22-Dec-2022	9.8	Mozilla developers Bryce Seager van Dyk and the Mozilla Fuzzing Team reported potential vulnerabilities present in Firefox 101. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 102. **CVE ID : CVE-2022-34485**	https://www.mozilla.org/security/advisories/mfsa2022-24/	A-MOZ-FIRE-090123/361
Product: firefox_esr					
Affected Version(s): * Up to (excluding) 102.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2022	6.1	When injecting an HTML base element, some requests would ignore the CSP's base-uri settings and accept the injected element's base instead. This vulnerability affects Firefox ESR < 102.3, Thunderbird < 102.3, and Firefox < 105. **CVE ID : CVE-2022-40956**	https://www.mozilla.org/security/advisories/mfsa2022-42/, https://www.mozilla.org/security/advisories/mfsa2022-41/, https://www.mozilla.org/security/advisories/mfsa2022-40/, https://bugzilla.mozilla.org/show_bug.cgi?id=1770094	A-MOZ-FIRE-090123/362
Out-of-bounds Read	22-Dec-2022	5.5	An out-of-bounds read can occur when decoding H264 video. This results in a potentially exploitable crash. This vulnerability affects Firefox ESR < 102.3, Thunderbird < 102.3, and Firefox < 105. **CVE ID : CVE-2022-3266**	https://www.mozilla.org/security/advisories/mfsa2022-42/, https://www.mozilla.org/security/advisories/mfsa2022-41/, https://www.mozilla.org/security/advisories/mfsa2022-40/, https://bugzilla.mozilla.org/show_bug.cgi?id=1767360	A-MOZ-FIRE-090123/363
Affected Version(s): * Up to (excluding) 91.11					
N/A	22-Dec-2022	8.8	An iframe that was not permitted to run scripts	https://www.mozilla.or	A-MOZ-FIRE-090123/364

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could do so if the user clicked on a <code>javascript:</code> link. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34468**	g/security/advisories/mfsa2022-24/, https://bugzilla.mozilla.org/show_bug.cgi?id=1768537, https://www.mozilla.org/security/advisories/mfsa2022-26/, https://www.mozilla.org/security/advisories/mfsa2022-25/	
Integer Overflow or Wraparound	22-Dec-2022	8.8	In the <code>nsTArray_Impl::ReplaceElementsAt()</code> function, an integer overflow could have occurred when the number of elements to replace was too large for the container. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34481**	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://bugzilla.mozilla.org/show_bug.cgi?id=1497246, https://www.mozilla.org/security/advisories/mfsa2022-26/, https://www.mozilla.org/security/advisories/mfsa2022-25/	A-MOZ-FIRE-090123/365
Reachable Assertion	22-Dec-2022	8.8	The Mozilla Fuzzing Team reported potential vulnerabilities present in Thunderbird 91.10. Some of these	https://www.mozilla.org/security/advisories/mfsa2022-24/,	A-MOZ-FIRE-090123/366

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34484**	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1763634%2C1772651, https://www.mozilla.org/security/advisories/mfsa2022-26/, https://www.mozilla.org/security/advisories/mfsa2022-25/	
N/A	22-Dec-2022	6.5	A malicious website that could create a popup could have resized the popup to overlay the address bar with its own content, resulting in potential user confusion or spoofing attacks. *This bug only affects Thunderbird for Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34479**	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://www.mozilla.org/security/advisories/mfsa2022-26/, https://www.mozilla.org/security/advisories/mfsa2022-25/, https://bugzilla.mozilla.org/show_bug.cgi?id=1745595	A-MOZ-FIRE-090123/367
Affected Version(s): * Up to (excluding) 91.13					
Out-of-bounds Write	22-Dec-2022	8.8	Members the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 103, Firefox ESR 102.1, and	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1770630%2C1	A-MOZ-FIRE-090123/368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR 91.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 102.2, Thunderbird < 91.13, Firefox ESR < 91.13, Firefox ESR < 102.2, and Firefox < 104. **CVE ID : CVE-2022-38478**	776658, https://www.mozilla.org/security/advisories/mfsa2022-35/, https://www.mozilla.org/security/advisories/mfsa2022-34/, https://www.mozilla.org/security/advisories/mfsa2022-33/	
Affected Version(s): * Up to (excluding) 91.5					
Out-of-bounds Write	22-Dec-2022	8.8	Applying a CSS filter effect could have accessed out of bounds memory. This could have lead to a heap-buffer-overflow causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22738**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/, https://bugzilla.mozilla.org/show_bug.cgi?id=1742382	A-MOZ-FIRE-090123/369
Use After Free	22-Dec-2022	8.8	Certain network request objects were freed too early when releasing a network request handle. This	https://www.mozilla.org/security/advisories/mfsa2022-02/,	A-MOZ-FIRE-090123/370

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could have lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22740**	https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1742334, https://www.mozilla.org/security/advisories/mfsa2022-03/	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Dec-2022	8.8	The constructed curl command from the "Copy as curl" feature in DevTools was not properly escaped for PowerShell. This could have lead to command injection if pasted into a Powershell prompt. *This bug only affects Thunderbird for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22744**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/371
Out-of-bounds Write	22-Dec-2022	8.8	Mozilla developers Calixte Denizet, Kershaw Chang, Christian Holler, Jason Kratzer, Gabriele Svelto, Tyson Smith, Simon Giesecke, and Steve	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.or	A-MOZ-FIRE-090123/372

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Fink reported memory safety bugs present in Firefox 95 and Firefox ESR 91.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22751**	g/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	
Use After Free	22-Dec-2022	7.5	Constructing audio sinks could have lead to a race condition when playing audio files and closing windows. This could have lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22737**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1745874, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/373
N/A	22-Dec-2022	7.5	When resizing a popup while requesting fullscreen access, the popup would have become unable to leave fullscreen mode. This	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://ww	A-MOZ-FIRE-090123/374

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22741**	w.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	
N/A	22-Dec-2022	6.5	Malicious websites could have tricked users into accepting launching a program to handle an external URL protocol. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22739**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1744158, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/375
Out-of-bounds Read	22-Dec-2022	6.5	When inserting text while in edit mode, some characters might have lead to out-of-bounds memory access causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22742**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/a	A-MOZ-FIRE-090123/376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				dvisories/mfsa2022-03/	
N/A	22-Dec-2022	6.5	Securitypolicyviolation events could have leaked cross-origin information for frame-ancestors violations. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22745**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/377
Improper Certificate Validation	22-Dec-2022	6.5	After accepting an untrusted certificate, handling an empty pkcs7 sequence as part of the certificate data could have lead to a crash. This crash is believed to be unexploitable. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22747**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1735028, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/378
N/A	22-Dec-2022	6.5	Malicious websites could have confused Firefox into showing the wrong origin when asking to launch a program and handling	https://bugzilla.mozilla.org/show_bug.cgi?id=1705211, https://ww	A-MOZ-FIRE-090123/379

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an external URL protocol. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22748**	w.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Dec-2022	5.9	A race condition could have allowed bypassing the fullscreen notification which could have lead to a fullscreen window spoof being unnoticed. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22746**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-FIRE-090123/380
N/A	22-Dec-2022	4.3	When navigating from inside an iframe while requesting fullscreen access, an attacker-controlled tab could have made the browser unable to leave fullscreen mode. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.or	A-MOZ-FIRE-090123/381

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-22743	g/security/advisories/mfsa2022-03/	
Affected Version(s): * Up to (excluding) 91.6					
N/A	22-Dec-2022	9.6	If a document created a sandboxed iframe without <code>allow-scripts</code>, and subsequently appended an element to the iframe's document that e.g. had a JavaScript event handler - the event handler would have run despite the iframe's sandbox. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22759**	https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/, https://bugzilla.mozilla.org/show_bug.cgi?id=1739957	A-MOZ-FIRE-090123/382
N/A	22-Dec-2022	8.8	If a user was convinced to drag and drop an image to their desktop or other folder, the resulting object could have been changed into an executable script which would have run arbitrary code after the user clicked on it. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22756**	https://bugzilla.mozilla.org/show_bug.cgi?id=1317873, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/a	A-MOZ-FIRE-090123/383

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				dvisories/mfsa2022-04/	
N/A	22-Dec-2022	8.8	Web-accessible extension pages (pages with a moz-extension:// scheme) were not correctly enforcing the frame-ancestors directive when it was used in the Web Extension's Content Security Policy. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22761**	https://bugzilla.mozilla.org/show_bug.cgi?id=1745566, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/384
N/A	22-Dec-2022	8.8	When a worker is shutdown, it was possible to cause script to run late in the lifecycle, at a point after where it should not be possible. This vulnerability affects Firefox < 96, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22763**	https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://bugzilla.mozilla.org/show_bug.cgi?id=1740534	A-MOZ-FIRE-090123/385

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Dec-2022	8.8	Mozilla developers Paul Adenot and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 96 and Firefox ESR 91.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22764**	https://www.mozilla.org/security/advisories/mfsa2022-06/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1742682%2C1744165%2C1746545%2C1748210%2C1748279, https://www.mozilla.org/security/advisories/mfsa2022-05/	A-MOZ-FIRE-090123/386
Time-of-check Time-of-use (TOCTOU) Race Condition	22-Dec-2022	7.1	A Time-of-Check Time-of-Use bug existed in the Maintenance (Updater) Service that could be abused to grant Users write access to an arbitrary directory. This could have been used to escalate to SYSTEM access. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22753**	https://bugzilla.mozilla.org/show_bug.cgi?id=1732435, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	22-Dec-2022	6.5	If a user installed an extension of a particular type, the extension could have auto-updated itself and while doing so, bypass the prompt which grants the new version the new requested permissions. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22754**	https://www.mozilla.org/security/advisories/mfsa2022-06/, https://bugzilla.mozilla.org/show_bug.cgi?id=1750565, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/388
Generation of Error Message Containing Sensitive Information	22-Dec-2022	6.5	When importing resources using Web Workers, error messages would distinguish the difference between <code>application/javascript</code> responses and non-script responses. This could have been abused to learn information cross-origin. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22760**	https://bugzilla.mozilla.org/show_bug.cgi?id=1748503, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-FIRE-090123/389
Affected Version(s): * Up to (excluding) 91.6.1					
Use After Free	22-Dec-2022	9.6	An unexpected message in the WebGPU IPC	https://bugzilla.mozilla.o	A-MOZ-FIRE-090123/390

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			framework could lead to a use-after-free and exploitable sandbox escape. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0. **CVE ID : CVE-2022-26486**	rg/show_bug.cgi?id=1758070, https://www.mozilla.org/security/advisories/mfsa2022-09/	
Use After Free	22-Dec-2022	8.8	Removing an XSLT parameter during processing could have lead to an exploitable use-after-free. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0. **CVE ID : CVE-2022-26485**	https://bugzilla.mozilla.org/show_bug.cgi?id=1758062, https://www.mozilla.org/security/advisories/mfsa2022-09/	A-MOZ-FIRE-090123/391
Affected Version(s): * Up to (excluding) 91.7					
N/A	22-Dec-2022	9.6	If an attacker could control the contents of an iframe sandboxed with <code>allow-popups</code> but not <code>allow-scripts</code>, they were able to craft a link that, when clicked, would lead to	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/,	A-MOZ-FIRE-090123/392

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			JavaScript execution in violation of the sandbox. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7. **CVE ID : CVE-2022-26384**	https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1744352	
Use After Free	22-Dec-2022	8.8	An attacker could have caused a use-after-free by forcing a text reflow in an SVG object leading to a potentially exploitable crash. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7. **CVE ID : CVE-2022-26381**	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/, https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1736243	A-MOZ-FIRE-090123/393
Time-of-check Time-of-use (TOCTOU) Race Condition	22-Dec-2022	7.5	When installing an add-on, Firefox verified the signature before prompting the user; but while the user was confirming the prompt, the underlying add-on file could have been modified and Firefox would not have noticed. This vulnerability affects Firefox < 98,	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/, https://www.mozilla.org/security/a	A-MOZ-FIRE-090123/394

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 91.7, and Thunderbird < 91.7. **CVE ID : CVE-2022-26387**	dvisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1752979	
N/A	22-Dec-2022	6.5	Previously Firefox for macOS and Linux would download temporary files to a user-specific directory in <code>/tmp</code>, but this behavior was changed to download them to <code>/tmp</code> where they could be affected by other local users. This behavior was reverted to the original, user-specific directory. *This bug only affects Firefox for macOS and Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.7 and Thunderbird < 91.7. **CVE ID : CVE-2022-26386**	https://bugzilla.mozilla.org/show_bug.cgi?id=1752396, https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/	A-MOZ-FIRE-090123/395
N/A	22-Dec-2022	4.3	When resizing a popup after requesting fullscreen access, the popup would not display the fullscreen notification. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7.	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/,	A-MOZ-FIRE-090123/396

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26383	https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1742421	
Affected Version(s): * Up to (excluding) 91.8					
Out-of-bounds Write	22-Dec-2022	8.8	If a compromised content process sent an unexpected number of WebAuthN Extensions in a Register command to the parent process, an out of bounds write would have occurred leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28281**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1755621, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/advisories/mfsa2022-14/	A-MOZ-FIRE-090123/397
Out-of-bounds Write	22-Dec-2022	8.8	Mozilla developers and community members Nika Layzell, Andrew McCreight, Gabriele Svelto, and the Mozilla Fuzzing Team reported memory safety bugs present in Thunderbird 91.7. Some of these bugs showed evidence of memory corruption and we presume that	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1663508%2C1744525%2C1753508%2	A-MOZ-FIRE-090123/398

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28289**	C1757476%2C1757805%2C1758549%2C1758776, https://www.mozilla.org/security/advisories/mfsa2022-15/	
Use After Free	22-Dec-2022	6.5	<code>NSSToken</code> objects were referenced via direct points, and could have been accessed in an unsafe way on different threads, leading to a use-after-free and potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-1097**	https://bugzilla.mozilla.org/show_bug.cgi?id=1745667, https://www.mozilla.org/security/advisories/mfsa2022-13/, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/advisories/mfsa2022-14/	A-MOZ-FIRE-090123/399
Use After Free	22-Dec-2022	6.5	After a VR Process is destroyed, a reference to it may have been retained and used, leading to a use-after-free and potentially exploitable crash. This vulnerability affects Thunderbird < 91.8 and Firefox ESR < 91.8. **CVE ID : CVE-2022-1196**	https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/advisories/mfsa2022-14/, https://bugzilla.mozilla.org/show_bu	A-MOZ-FIRE-090123/400

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				g.cgi?id=1750679	
Use After Free	22-Dec-2022	6.5	By using a link with <code>rel="localization "</code> a use-after-free could have been triggered by destroying an object during JavaScript execution and then referencing the object through a freed pointer, leading to a potential exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28282**	https://bugzilla.mozilla.org/show_bug.cgi?id=1751609, https://www.mozilla.org/security/advisories/mfsa2022-13/, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/advisories/mfsa2022-14/	A-MOZ-FIRE-090123/401
N/A	22-Dec-2022	6.5	When generating the assembly code for <code>MLoadTypedArrayElementHole</code>, an incorrect AliasSet was used. In conjunction with another vulnerability this could have been used for an out of bounds memory read. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28285**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://bugzilla.mozilla.org/show_bug.cgi?id=1756957, https://www.mozilla.org/security/advisories/mfsa2022-14/	A-MOZ-FIRE-090123/402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Rendered UI Layers or Frames	22-Dec-2022	5.4	Due to a layout change, iframe contents could have been rendered outside of its border. This could have led to user confusion or spoofing attacks. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28286**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1735265, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/advisories/mfsa2022-14/	A-MOZ-FIRE-090123/403
Affected Version(s): * Up to (excluding) 91.9					
Reachable Assertion	22-Dec-2022	9.8	Mozilla developers Andrew McCreight, Gabriele Svelto, Tom Ritter and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 99 and Firefox ESR 91.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100. **CVE ID : CVE-2022-29917**	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1684739%2C1706441%2C1753298%2C1762614%2C1762620%2C1764778, https://www.mozilla.org/security/advisories/mfsa2022-17/, https://www.mozilla.org/security/advisories/mfsa2022-16/	A-MOZ-FIRE-090123/404

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	22-Dec-2022	8.8	Documents in deeply-nested cross-origin browsing contexts could have obtained permissions granted to the top-level origin, bypassing the existing prompt and wrongfully inheriting the top-level permissions. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100. **CVE ID : CVE-2022-29909**	https://www.mozilla.org/security/advisories/mfsa2022-17/, https://www.mozilla.org/security/advisories/mfsa2022-16/, https://bugzilla.mozilla.org/show_bug.cgi?id=1755081	A-MOZ-FIRE-090123/405
N/A	22-Dec-2022	6.5	Firefox behaved slightly differently for already known resources when loading CSS resources involving CSS variables. This could have been used to probe the browser history. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100. **CVE ID : CVE-2022-29916**	https://bugzilla.mozilla.org/show_bug.cgi?id=1760674, https://www.mozilla.org/security/advisories/mfsa2022-17/, https://www.mozilla.org/security/advisories/mfsa2022-16/, https://www.mozilla.org/security/advisories/mfsa2022-18/	A-MOZ-FIRE-090123/406
Affected Version(s): * Up to (excluding) 91.9.1					
Improperly Controlled Modification of Object Prototype Attributes	22-Dec-2022	8.8	An attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object,	https://bugzilla.mozilla.org/show_bug.cgi?id=1770048, https://ww	A-MOZ-FIRE-090123/407

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Prototype Pollution')			leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1. **CVE ID : CVE-2022-1529**	w.mozilla.org/security/advisories/mfsa2022-19/	
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	22-Dec-2022	8.8	If an attacker was able to corrupt the methods of an Array object in JavaScript via prototype pollution, they could have achieved execution of attacker-controlled JavaScript code in a privileged context. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1. **CVE ID : CVE-2022-1802**	https://bugzilla.mozilla.org/show_bug.cgi?id=1770137, https://www.mozilla.org/security/advisories/mfsa2022-19/	A-MOZ-FIRE-090123/408
Affected Version(s): From (including) 102.0 Up to (excluding) 102.2					
Out-of-bounds Write	22-Dec-2022	8.8	Members the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 103, Firefox ESR 102.1, and Firefox ESR 91.12. Some of these bugs showed evidence of memory corruption and	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1770630%2C1776658, https://www.mozilla.org/security/a	A-MOZ-FIRE-090123/409

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 102.2, Thunderbird < 91.13, Firefox ESR < 91.13, Firefox ESR < 102.2, and Firefox < 104. **CVE ID : CVE-2022-38478**	dvisories/mfsa2022-35/, https://www.mozilla.org/security/advisories/mfsa2022-34/, https://www.mozilla.org/security/advisories/mfsa2022-33/	
Product: firefox_focus					
Affected Version(s): * Up to (excluding) 97.3.0					
Use After Free	22-Dec-2022	9.6	An unexpected message in the WebGPU IPC framework could lead to a use-after-free and exploitable sandbox escape. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0. **CVE ID : CVE-2022-26486**	https://bugzilla.mozilla.org/show_bug.cgi?id=1758070, https://www.mozilla.org/security/advisories/mfsa2022-09/	A-MOZ-FIRE-090123/410
Use After Free	22-Dec-2022	8.8	Removing an XSLT parameter during processing could have lead to an exploitable use-after-free. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1,	https://bugzilla.mozilla.org/show_bug.cgi?id=1758062, https://www.mozilla.org/security/advisories/mfsa2022-09/	A-MOZ-FIRE-090123/411

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0. **CVE ID : CVE-2022-26485**		
Product: thunderbird					
Affected Version(s): * Up to (excluding) 102.3					
N/A	22-Dec-2022	7.8	When saving or opening an email attachment on macOS, Thunderbird did not set attribute com.apple.quarantine on the received file. If the received file was an application and the user attempted to open it, then the application was started immediately without asking the user to confirm. This vulnerability affects Thunderbird < 102.3. **CVE ID : CVE-2022-3155**	https://www.mozilla.org/security/advisories/mfsa2022-42/, https://bugzilla.mozilla.org/show_bug.cgi?id=1789061	A-MOZ-THUN-090123/412
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2022	6.1	When injecting an HTML base element, some requests would ignore the CSP's base-uri settings and accept the injected element's base instead. This vulnerability affects Firefox ESR < 102.3, Thunderbird < 102.3, and Firefox < 105. **CVE ID : CVE-2022-40956**	https://www.mozilla.org/security/advisories/mfsa2022-42/, https://www.mozilla.org/security/advisories/mfsa2022-41/, https://www.mozilla.org/security/advisories/mfsa2022-40/,	A-MOZ-THUN-090123/413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				https://bugzilla.mozilla.org/show_bug.cgi?id=1770094	
Out-of-bounds Read	22-Dec-2022	5.5	An out-of-bounds read can occur when decoding H264 video. This results in a potentially exploitable crash. This vulnerability affects Firefox ESR < 102.3, Thunderbird < 102.3, and Firefox < 105. **CVE ID : CVE-2022-3266**	https://www.mozilla.org/security/advisories/mfsa2022-42/, https://www.mozilla.org/security/advisories/mfsa2022-41/, https://www.mozilla.org/security/advisories/mfsa2022-40/, https://bugzilla.mozilla.org/show_bug.cgi?id=1767360	A-MOZ-THUN-090123/414
Affected Version(s): * Up to (excluding) 91.11					
N/A	22-Dec-2022	8.8	An iframe that was not permitted to run scripts could do so if the user clicked on a <code>javascript:</code> link. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34468**	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://bugzilla.mozilla.org/show_bug.cgi?id=1768537, https://www.mozilla.org/security/advisories/mfsa2022-26/, https://www.mozilla.or	A-MOZ-THUN-090123/415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				g/security/advisories/mfsa2022-25/	
Integer Overflow or Wraparound	22-Dec-2022	8.8	In the <code>nsTArray_Impl::ReplaceElementsAt()</code> function, an integer overflow could have occurred when the number of elements to replace was too large for the container. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34481**	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://bugzilla.mozilla.org/show_bug.cgi?id=1497246, https://www.mozilla.org/security/advisories/mfsa2022-26/, https://www.mozilla.org/security/advisories/mfsa2022-25/	A-MOZ-THUN-090123/416
Reachable Assertion	22-Dec-2022	8.8	The Mozilla Fuzzing Team reported potential vulnerabilities present in Thunderbird 91.10. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34484**	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1763634%2C1772651, https://www.mozilla.org/security/advisories/mfsa2022-26/, https://www.mozilla.org/security/a	A-MOZ-THUN-090123/417

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				dvisories/mfsa2022-25/	
N/A	22-Dec-2022	6.5	A malicious website that could create a popup could have resized the popup to overlay the address bar with its own content, resulting in potential user confusion or spoofing attacks. *This bug only affects Thunderbird for Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34479**	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://www.mozilla.org/security/advisories/mfsa2022-26/, https://www.mozilla.org/security/advisories/mfsa2022-25/, https://bugzilla.mozilla.org/show_bug.cgi?id=1745595	A-MOZ-THUN-090123/418
Affected Version(s): * Up to (excluding) 91.13					
Out-of-bounds Write	22-Dec-2022	8.8	Members the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 103, Firefox ESR 102.1, and Firefox ESR 91.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 102.2, Thunderbird < 91.13, Firefox ESR < 91.13,	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1770630%2C1776658, https://www.mozilla.org/security/advisories/mfsa2022-35/, https://www.mozilla.org/security/advisories/mfsa2022-34/, https://www.mozilla.org/security/a	A-MOZ-THUN-090123/419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 102.2, and Firefox < 104. **CVE ID : CVE-2022-38478**	dvisories/mfsa2022-33/	
Affected Version(s): * Up to (excluding) 91.5					
Out-of-bounds Write	22-Dec-2022	8.8	Applying a CSS filter effect could have accessed out of bounds memory. This could have lead to a heap-buffer-overflow causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22738**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/, https://bugzilla.mozilla.org/show_bug.cgi?id=1742382	A-MOZ-THUN-090123/420
Use After Free	22-Dec-2022	8.8	Certain network request objects were freed too early when releasing a network request handle. This could have lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22740**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1742334, https://www.mozilla.org/security/a	A-MOZ-THUN-090123/421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				dvisories/mfsa2022-03/	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Dec-2022	8.8	The constructed curl command from the "Copy as curl" feature in DevTools was not properly escaped for PowerShell. This could have lead to command injection if pasted into a Powershell prompt. *This bug only affects Thunderbird for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22744**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-THUN-090123/422
Out-of-bounds Write	22-Dec-2022	8.8	Mozilla developers Calixte Denizet, Kershaw Chang, Christian Holler, Jason Kratzer, Gabriele Svelto, Tyson Smith, Simon Giesecke, and Steve Fink reported memory safety bugs present in Firefox 95 and Firefox ESR 91.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 91.5,	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-THUN-090123/423

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22751**		
Use After Free	22-Dec-2022	7.5	Constructing audio sinks could have lead to a race condition when playing audio files and closing windows. This could have lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22737**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1745874, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-THUN-090123/424
N/A	22-Dec-2022	7.5	When resizing a popup while requesting fullscreen access, the popup would have become unable to leave fullscreen mode. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22741**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-THUN-090123/425
N/A	22-Dec-2022	6.5	Malicious websites could have tricked users into accepting launching a program to	https://www.mozilla.org/security/advisories/mf	A-MOZ-THUN-090123/426

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			handle an external URL protocol. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22739**	sa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1744158, https://www.mozilla.org/security/advisories/mfsa2022-03/	
Out-of-bounds Read	22-Dec-2022	6.5	When inserting text while in edit mode, some characters might have lead to out-of-bounds memory access causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22742**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-THUN-090123/427
N/A	22-Dec-2022	6.5	Securitypolicyviolation events could have leaked cross-origin information for frame-ancestors violations. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22745**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.or	A-MOZ-THUN-090123/428

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				g/security/advisories/mfsa2022-03/	
Improper Certificate Validation	22-Dec-2022	6.5	After accepting an untrusted certificate, handling an empty pkcs7 sequence as part of the certificate data could have lead to a crash. This crash is believed to be unexploitable. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22747**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1735028, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-THUN-090123/429
N/A	22-Dec-2022	6.5	Malicious websites could have confused Firefox into showing the wrong origin when asking to launch a program and handling an external URL protocol. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22748**	https://bugzilla.mozilla.org/show_bug.cgi?id=1705211, https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-THUN-090123/430

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Dec-2022	5.9	A race condition could have allowed bypassing the fullscreen notification which could have lead to a fullscreen window spoof being unnoticed. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22746**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-THUN-090123/431
N/A	22-Dec-2022	4.3	When navigating from inside an iframe while requesting fullscreen access, an attacker-controlled tab could have made the browser unable to leave fullscreen mode. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22743**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	A-MOZ-THUN-090123/432
Affected Version(s): * Up to (excluding) 91.6					
N/A	22-Dec-2022	9.6	If a document created a sandboxed iframe without <code>allow-scripts</code>, and subsequently appended an element to the iframe's document that e.g. had a JavaScript event handler - the event handler would	https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/,	A-MOZ-THUN-090123/433

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			have run despite the iframe's sandbox. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22759**	https://www.mozilla.org/security/advisories/mfsa2022-04/, https://bugzilla.mozilla.org/show_bug.cgi?id=1739957	
N/A	22-Dec-2022	8.8	If a user was convinced to drag and drop an image to their desktop or other folder, the resulting object could have been changed into an executable script which would have run arbitrary code after the user clicked on it. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22756**	https://bugzilla.mozilla.org/show_bug.cgi?id=1317873, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-THUN-090123/434
N/A	22-Dec-2022	8.8	Web-accessible extension pages (pages with a moz-extension:// scheme) were not correctly enforcing the frame-ancestors directive when it was used in the Web Extension's Content Security Policy. This vulnerability affects Firefox < 97,	https://bugzilla.mozilla.org/show_bug.cgi?id=1745566, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/a	A-MOZ-THUN-090123/435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22761**	dvisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	
N/A	22-Dec-2022	8.8	When a worker is shutdown, it was possible to cause script to run late in the lifecycle, at a point after where it should not be possible. This vulnerability affects Firefox < 96, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22763**	https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://bugzilla.mozilla.org/show_bug.cgi?id=1740534	A-MOZ-THUN-090123/436
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Dec-2022	8.8	Mozilla developers Paul Adenot and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 96 and Firefox ESR 91.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 97,	https://www.mozilla.org/security/advisories/mfsa2022-06/, https://bugzilla.mozilla.org/buglist.cgi?bug_id=1742682%2C1744165%2C1746545%2C1748210%2C1748279, https://www.mozilla.or	A-MOZ-THUN-090123/437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22764**	g/security/advisories/mfsa2022-05/	
Time-of-check Time-of-use (TOCTOU) Race Condition	22-Dec-2022	7.1	A Time-of-Check Time-of-Use bug existed in the Maintenance (Updater) Service that could be abused to grant Users write access to an arbitrary directory. This could have been used to escalate to SYSTEM access. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22753**	https://bugzilla.mozilla.org/show_bug.cgi?id=1732435, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-THUN-090123/438
Incorrect Authorization	22-Dec-2022	6.5	If a user installed an extension of a particular type, the extension could have auto-updated itself and while doing so, bypass the prompt which grants the new version the new requested permissions. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22754**	https://www.mozilla.org/security/advisories/mfsa2022-06/, https://bugzilla.mozilla.org/show_bug.cgi?id=1750565, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/a	A-MOZ-THUN-090123/439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				dvisories/mfsa2022-04/	
Generation of Error Message Containing Sensitive Information	22-Dec-2022	6.5	When importing resources using Web Workers, error messages would distinguish the difference between <code>application/javascript</code> responses and non-script responses. This could have been abused to learn information cross-origin. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22760**	https://bugzilla.mozilla.org/show_bug.cgi?id=1748503, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	A-MOZ-THUN-090123/440
Affected Version(s): * Up to (excluding) 91.6.1					
Out-of-bounds Write	22-Dec-2022	8.8	It may be possible for an attacker to craft an email message that causes Thunderbird to perform an out-of-bounds write of one byte when processing the message. This vulnerability affects Thunderbird < 91.6.1. **CVE ID : CVE-2022-0566**	https://bugzilla.mozilla.org/show_bug.cgi?id=1753094, https://www.mozilla.org/security/advisories/mfsa2022-07/	A-MOZ-THUN-090123/441
Affected Version(s): * Up to (excluding) 91.7					
N/A	22-Dec-2022	9.6	If an attacker could control the contents of an iframe sandboxed with <code>allow-popups</code> but not <code>allow-	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://ww	A-MOZ-THUN-090123/442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			scripts</code>, they were able to craft a link that, when clicked, would lead to JavaScript execution in violation of the sandbox. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7. **CVE ID : CVE-2022-26384**	w.mozilla.org/security/advisories/mfsa2022-11/, https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1744352	
Use After Free	22-Dec-2022	8.8	An attacker could have caused a use-after-free by forcing a text reflow in an SVG object leading to a potentially exploitable crash. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7. **CVE ID : CVE-2022-26381**	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/, https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1736243	A-MOZ-THUN-090123/443
Time-of-check Time-of-use (TOCTOU) Race Condition	22-Dec-2022	7.5	When installing an add-on, Firefox verified the signature before prompting the user; but while the user was confirming the prompt, the underlying add-on file could have been modified and Firefox	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mf	A-MOZ-THUN-090123/444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would not have noticed. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7. **CVE ID : CVE-2022-26387**	sa2022-11/, https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1752979	
N/A	22-Dec-2022	6.5	Previously Firefox for macOS and Linux would download temporary files to a user-specific directory in <code>/tmp</code>, but this behavior was changed to download them to <code>/tmp</code> where they could be affected by other local users. This behavior was reverted to the original, user-specific directory. *This bug only affects Firefox for macOS and Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.7 and Thunderbird < 91.7. **CVE ID : CVE-2022-26386**	https://bugzilla.mozilla.org/show_bug.cgi?id=1752396, https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/	A-MOZ-THUN-090123/445
N/A	22-Dec-2022	4.3	When resizing a popup after requesting fullscreen access, the popup would not display the fullscreen notification. This	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://ww	A-MOZ-THUN-090123/446

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7. **CVE ID : CVE-2022-26383**	w.mozilla.org/security/advisories/mfsa2022-11/, https://www.mozilla.org/security/advisories/mfsa2022-10/, https://bugzilla.mozilla.org/show_bug.cgi?id=1742421	
Affected Version(s): * Up to (excluding) 91.8					
Out-of-bounds Write	22-Dec-2022	8.8	If a compromised content process sent an unexpected number of WebAuthN Extensions in a Register command to the parent process, an out of bounds write would have occurred leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28281**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1755621, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/advisories/mfsa2022-14/	A-MOZ-THUN-090123/447
Out-of-bounds Write	22-Dec-2022	8.8	Mozilla developers and community members Nika Layzell, Andrew McCreight, Gabriele Svelto, and the Mozilla Fuzzing Team reported memory safety bugs present in Thunderbird	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/buglist.cg	A-MOZ-THUN-090123/448

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			91.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28289**	i?bug_id=1663508%2C1744525%2C1753508%2C1757476%2C1757805%2C1758549%2C1758776, https://www.mozilla.org/security/advisories/mfsa2022-15/	
Use After Free	22-Dec-2022	6.5	<code>NSSToken</code> objects were referenced via direct points, and could have been accessed in an unsafe way on different threads, leading to a use-after-free and potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-1097**	https://bugzilla.mozilla.org/show_bug.cgi?id=1745667, https://www.mozilla.org/security/advisories/mfsa2022-13/, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/advisories/mfsa2022-14/	A-MOZ-THUN-090123/449
Use After Free	22-Dec-2022	6.5	After a VR Process is destroyed, a reference to it may have been retained and used, leading to a use-after-free and potentially exploitable crash. This vulnerability affects	https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/advisories/mf	A-MOZ-THUN-090123/450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 91.8 and Firefox ESR < 91.8. **CVE ID : CVE-2022-1196**	sa2022-14/, https://bugzilla.mozilla.org/show_bug.cgi?id=1750679	
Use After Free	22-Dec-2022	6.5	By using a link with <code>rel="localization"</code> a use-after-free could have been triggered by destroying an object during JavaScript execution and then referencing the object through a freed pointer, leading to a potential exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28282**	https://bugzilla.mozilla.org/show_bug.cgi?id=1751609, https://www.mozilla.org/security/advisories/mfsa2022-13/, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/advisories/mfsa2022-14/	A-MOZ-THUN-090123/451
N/A	22-Dec-2022	6.5	When generating the assembly code for <code>MLoadTypedArrayElementHole</code>, an incorrect AliasSet was used. In conjunction with another vulnerability this could have been used for an out of bounds memory read. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28285**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://bugzilla.mozilla.org/show_bug.cgi?id=1756957, https://www.mozilla.or	A-MOZ-THUN-090123/452

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				g/security/advisories/mfsa2022-14/	
Improper Certificate Validation	22-Dec-2022	5.4	When importing a revoked key that specified key compromise as the revocation reason, Thunderbird did not update the existing copy of the key that was not yet revoked, and the existing key was kept as non-revoked. Revocation statements that used another revocation reason, or that didn't specify a revocation reason, were unaffected. This vulnerability affects Thunderbird < 91.8. **CVE ID : CVE-2022-1197**	https://bugzilla.mozilla.org/show_bug.cgi?id=1754985, https://www.mozilla.org/security/advisories/mfsa2022-15/	A-MOZ-THUN-090123/453
Improper Restriction of Rendered UI Layers or Frames	22-Dec-2022	5.4	Due to a layout change, iframe contents could have been rendered outside of its border. This could have led to user confusion or spoofing attacks. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8. **CVE ID : CVE-2022-28286**	https://www.mozilla.org/security/advisories/mfsa2022-13/, https://bugzilla.mozilla.org/show_bug.cgi?id=1735265, https://www.mozilla.org/security/advisories/mfsa2022-15/, https://www.mozilla.org/security/a	A-MOZ-THUN-090123/454

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				dvisories/mfsa2022-14/	
Affected Version(s): * Up to (excluding) 91.9					
Reachable Assertion	22-Dec-2022	9.8	Mozilla developers Andrew McCreight, Gabriele Svelto, Tom Ritter and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 99 and Firefox ESR 91.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100. **CVE ID : CVE-2022-29917**	https://bugzilla.mozilla.org/buglist.cgi?bug_id=1684739%2C1706441%2C1753298%2C1762614%2C1762620%2C1764778, https://www.mozilla.org/security/advisories/mfsa2022-17/, https://www.mozilla.org/security/advisories/mfsa2022-16/	A-MOZ-THUN-090123/455
Incorrect Default Permissions	22-Dec-2022	8.8	Documents in deeply-nested cross-origin browsing contexts could have obtained permissions granted to the top-level origin, bypassing the existing prompt and wrongfully inheriting the top-level permissions. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100. **CVE ID : CVE-2022-29909**	https://www.mozilla.org/security/advisories/mfsa2022-17/, https://www.mozilla.org/security/advisories/mfsa2022-16/, https://bugzilla.mozilla.org/show_bug.cgi?id=1755081	A-MOZ-THUN-090123/456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	22-Dec-2022	6.5	Firefox behaved slightly differently for already known resources when loading CSS resources involving CSS variables. This could have been used to probe the browser history. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100. **CVE ID : CVE-2022-29916**	https://bugzilla.mozilla.org/show_bug.cgi?id=1760674, https://www.mozilla.org/security/advisories/mfsa2022-17/, https://www.mozilla.org/security/advisories/mfsa2022-16/, https://www.mozilla.org/security/advisories/mfsa2022-18/	A-MOZ-THUN-090123/457
Inadequate Encryption Strength	22-Dec-2022	4.3	When viewing an email message A, which contains an attached message B, where B is encrypted or digitally signed or both, Thunderbird may show an incorrect encryption or signature status. After opening and viewing the attached message B, when returning to the display of message A, the message A might be shown with the security status of message B. This vulnerability affects Thunderbird < 91.9. **CVE ID : CVE-2022-1520**	https://bugzilla.mozilla.org/show_bug.cgi?id=1745019, https://www.mozilla.org/security/advisories/mfsa2022-18/	A-MOZ-THUN-090123/458
Affected Version(s): * Up to (excluding) 91.9.1					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	22-Dec-2022	8.8	An attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1. **CVE ID : CVE-2022-1529**	https://bugzilla.mozilla.org/show_bug.cgi?id=1770048, https://www.mozilla.org/security/advisories/mfsa2022-19/	A-MOZ-THUN-090123/459
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	22-Dec-2022	8.8	If an attacker was able to corrupt the methods of an Array object in JavaScript via prototype pollution, they could have achieved execution of attacker-controlled JavaScript code in a privileged context. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1. **CVE ID : CVE-2022-1802**	https://bugzilla.mozilla.org/show_bug.cgi?id=1770137, https://www.mozilla.org/security/advisories/mfsa2022-19/	A-MOZ-THUN-090123/460
Affected Version(s): From (including) 102.0 Up to (excluding) 102.2					
Out-of-bounds Write	22-Dec-2022	8.8	Members the Mozilla Fuzzing Team reported memory safety bugs	https://bugzilla.mozilla.org/buglist.cg	A-MOZ-THUN-090123/461

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			present in Firefox 103, Firefox ESR 102.1, and Firefox ESR 91.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 102.2, Thunderbird < 91.13, Firefox ESR < 91.13, Firefox ESR < 102.2, and Firefox < 104. **CVE ID : CVE-2022-38478**	i?bug_id=1770630%2C1776658, https://www.mozilla.org/security/advisories/mfsa2022-35/, https://www.mozilla.org/security/advisories/mfsa2022-34/, https://www.mozilla.org/security/advisories/mfsa2022-33/	
Affected Version(s): * Up to (excluding) 91.10					
Improper Certificate Validation	22-Dec-2022	6.5	When displaying the sender of an email, and the sender name contained the Braille Pattern Blank space character multiple times, Thunderbird would have displayed all the spaces. This could have been used by an attacker to send an email message with the attacker's digital signature, that was shown with an arbitrary sender email address chosen by the attacker. If the sender name started with a false email address, followed by many Braille space characters, the	https://www.mozilla.org/security/advisories/mfsa2022-22/, https://bugzilla.mozilla.org/show_bug.cgi?id=1767816	A-MOZ-THUN-090123/462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker's email address was not visible. Because Thunderbird compared the invisible sender address with the signature's email address, if the signing key or certificate was accepted by Thunderbird, the email was shown as having a valid digital signature. This vulnerability affects Thunderbird < 91.10. **CVE ID : CVE-2022-1834**		
Affected Version(s): * Up to (excluding) 91.31.1					
Improper Restriction of Rendered UI Layers or Frames	22-Dec-2022	4.3	When receiving an HTML email that specified to load an <code>iframe</code> element from a remote location, a request to the remote document was sent. However, Thunderbird didn't display the document. This vulnerability affects Thunderbird < 102.2.1 and Thunderbird < 91.13.1. **CVE ID : CVE-2022-3034**	https://bugzilla.mozilla.org/show_bug.cgi?id=1745751, https://www.mozilla.org/security/advisories/mfsa2022-39/, https://www.mozilla.org/security/advisories/mfsa2022-38/	A-MOZ-THUN-090123/463
Affected Version(s): * Up to (excluding) 91.6.2					
Use After Free	22-Dec-2022	9.6	An unexpected message in the WebGPU IPC framework could lead to a use-after-free and exploitable sandbox escape. We have had reports of attacks in the	https://bugzilla.mozilla.org/show_bug.cgi?id=1758070, https://www.mozilla.or	A-MOZ-THUN-090123/464

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0. **CVE ID : CVE-2022-26486**	g/security/advisories/mfsa2022-09/	
Use After Free	22-Dec-2022	8.8	Removing an XSLT parameter during processing could have lead to an exploitable use-after-free. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0. **CVE ID : CVE-2022-26485**	https://bugzilla.mozilla.org/show_bug.cgi?id=1758062, https://www.mozilla.org/security/advisories/mfsa2022-09/	A-MOZ-THUN-090123/465
Affected Version(s): From (including) 102.0 Up to (excluding) 102.2.1					
Improper Restriction of Rendered UI Layers or Frames	22-Dec-2022	4.3	When receiving an HTML email that specified to load an <code>iframe</code> element from a remote location, a request to the remote document was sent. However, Thunderbird didn't display the document. This vulnerability affects Thunderbird < 102.2.1 and Thunderbird < 91.13.1.	https://bugzilla.mozilla.org/show_bug.cgi?id=1745751, https://www.mozilla.org/security/advisories/mfsa2022-39/, https://www.mozilla.org/security/advisories/mfsa2022-38/	A-MOZ-THUN-090123/466

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3034		
Product: vpn					
Affected Version(s): * Up to (excluding) 2.7.1					
Unrestricted Upload of File with Dangerous Type	22-Dec-2022	7.8	Mozilla VPN can load an OpenSSL configuration file from an unsecured directory. A user or attacker with limited privileges could leverage this to launch arbitrary code with SYSTEM privilege. This vulnerability affects Mozilla VPN < 2.7.1. **CVE ID : CVE-2022-0517**	https://bugzilla.mozilla.org/show_bug.cgi?id=1752291, https://www.mozilla.org/security/advisories/mfsa2022-08/	A-MOZ-VPN-090123/467
Vendor: Mutiny					
Product: mutiny					
Affected Version(s): * Up to (excluding) 7.2.0-10855					
Use of Hard-coded Credentials	16-Dec-2022	9.8	Mutiny 7.2.0-10788 suffers from Hardcoded root password. **CVE ID : CVE-2022-37832**	N/A	A-MUT-MUTI-090123/468
Vendor: nbnbk_project					
Product: nbnbk					
Affected Version(s): -					
Unrestricted Upload of File with Dangerous Type	22-Dec-2022	9.8	Default version of nbnbk was discovered to contain an arbitrary file upload vulnerability via the component /api/User/download_img. **CVE ID : CVE-2022-46493**	N/A	A-NBN-NBNB-090123/469

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	22-Dec-2022	6.5	A Cross-Site Request Forgery (CSRF) vulnerability in the Add Administrator function of the default version of nbnbk allows attackers to arbitrarily add Administrator accounts. **CVE ID : CVE-2022-46491**	N/A	A-NBN-NBNB-090123/470
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Dec-2022	6.5	nbnbk commit 879858451d53261d10f77d4709aee2d01c72c301 was discovered to contain an arbitrary file read vulnerability via the component /api/Index/getFileBinary. **CVE ID : CVE-2022-46492**	N/A	A-NBN-NBNB-090123/471
Vendor: ndk-design					
Product: ndkadvancedcustomizationfields					
Affected Version(s): * Up to (including) 3.5.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2022	6.1	A cross-site scripting (XSS) vulnerability in NdkAdvancedCustomizationFields v3.5.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payloads injected into the "htmlNodes" parameter. **CVE ID : CVE-2022-40841**	N/A	A-NDK-NDKA-090123/472
Vendor: Netapp					
Product: oncommand_insight					
Affected Version(s): From (including) 7.3.1 Up to (including) 7.3.14					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	20-Dec-2022	8.6	OnCommand Insight versions 7.3.1 through 7.3.14 are susceptible to an authentication bypass vulnerability in the Data Warehouse component. **CVE ID : CVE-2022-38733**	https://security.netapp.com/advisory/NTAP-20221220-0001/	A-NET-ONCO-090123/473
Vendor: noorsplugin					
Product: checkout_for_paypal					
Affected Version(s): * Up to (excluding) 1.0.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	The Checkout for PayPal WordPress plugin before 1.0.14 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2022-3983**	N/A	A-NOO-CHEC-090123/474
Product: easy_video_player					
Affected Version(s): * Up to (excluding) 1.2.2.3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	The Easy Video Player WordPress plugin before 1.2.2.3 does not sanitize and escapes some parameters, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.	N/A	A-NOO-EASY-090123/475

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3937		
Product: responsive_lightbox2					
Affected Version(s): * Up to (excluding) 1.0.4					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	The Responsive Lightbox2 WordPress plugin before 1.0.4 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2022-3987**	N/A	A-NOO-RESP-090123/476
Product: wp_stripe_checkout					
Affected Version(s): * Up to (excluding) 1.2.2.21					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	The WP Stripe Checkout WordPress plugin before 1.2.2.21 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2022-3986**	N/A	A-NOO-WP_S-090123/477
Vendor: oc-server3_project					
Product: oc-server3					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-2022	6.1	A vulnerability classified as problematic has been found in Opencaching Deutschland oc-server3. This affects an unknown part of the file htdocs/templates2/ocstyle/start.tpl of the component Cookie Handler. The manipulation of the argument usercountryCode leads to cross site scripting. It is possible to initiate the attack remotely. The name of the patch is c720f2777a452186c67ef30db3679dd409556544. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216171. **CVE ID : CVE-2022-4585**	https://github.com/OpencachingDeutschland/oc-server3/commit/c720f2777a452186c67ef30db3679dd409556544, https://github.com/OpencachingDeutschland/oc-server3/pull/894	A-OC--OC-S-090123/478
Affected Version(s): * Up to (excluding) 2022-09-04					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-2022	6.1	A vulnerability classified as problematic was found in Opencaching Deutschland oc-server3. This vulnerability affects unknown code of the file htdocs/templates2/ocstyle/cachelists.tpl of the component Cachelist Handler. The	https://github.com/OpencachingDeutschland/oc-server3/commit/a9f79c7da78cd24a7ef1d298e6bc86006972ea73, https://github.com/OpencachingDeu	A-OC--OC-S-090123/479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			manipulation of the argument name_filter/by_filter leads to cross site scripting. The attack can be initiated remotely. The name of the patch is a9f79c7da78cd24a7ef1d298e6bc86006972ea73. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216172. **CVE ID : CVE-2022-4586**	tschland/oc-server3/pull/894	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-2022	5.4	A vulnerability, which was classified as problematic, has been found in Opencaching Deutschland oc-server3. This issue affects some unknown processing of the file htdocs/templates2/ocstyle/login.tpl of the component Login Page. The manipulation of the argument username leads to cross site scripting. The attack may be initiated remotely. The name of the patch is 3296ebd61e7fe49e93b5755d5d7766d6e94a7667. It is recommended to apply a patch to fix this issue. The identifier VDB-216173 was assigned to this vulnerability.	https://github.com/OpencachingDeutschland/oc-server3/commit/3296ebd61e7fe49e93b5755d5d7766d6e94a7667, https://github.com/OpencachingDeutschland/oc-server3/pull/893	A-OC--OC-S-090123/480

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-4587		
Vendor: Omron					
Product: cx-drive					
Affected Version(s): * Up to (including) 3.00					
Use After Free	21-Dec-2022	7.8	Use after free vulnerability in CX-Drive V3.00 and earlier allows a local attacker to execute arbitrary code by having a user to open a specially crafted file, **CVE ID : CVE-2022-46282**	N/A	A-OMR-CX-D-090123/481
Vendor: Open-emr					
Product: openemr					
Affected Version(s): * Up to (excluding) 7.0.0.2					
Improper Access Control	17-Dec-2022	8.1	Improper Access Control in GitHub repository openemr/openemr prior to 7.0.0.2. **CVE ID : CVE-2022-4567**	https://hunt r.dev/bounti es/1ac677c4 -ec0a-4788-9465-51d9b6bd8fd2, https://gith ub.com/ope nemr/opene mr/commit/953cb84dfd55fee9d5296668ec7fdb8bf25bcea4	A-OPE-OPEN-090123/482
Improper Neutralization of Input During Web Page Generation	19-Dec-2022	6.1	Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.2. **CVE ID : CVE-2022-4615**	https://hunt r.dev/bounti es/9c66ece4 -bcaa-417d-8b98-e8daff8a728b,	A-OPE-OPEN-090123/483

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				https://github.com/openemr/openemr/commit/d5eb41697f7f1bc2c7ee5bc9bbf58684e1c8cc14	
Vendor: openimageio					
Product: openimageio					
Affected Version(s): 2.3.19.0					
Out-of-bounds Read	22-Dec-2022	3.3	An out of bounds read vulnerability exists in the way OpenImageIO version v2.3.19.0 processes string fields in TIFF image files. A specially-crafted TIFF file can lead to information disclosure. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-41977**	N/A	A-OPE-OPEN-090123/484
Affected Version(s): 2022-09-14					
Out-of-bounds Read	22-Dec-2022	5.5	A heap out of bounds read vulnerability exists in the OpenImageIO master-branch-9aeece7a when parsing the image file directory part of a PSD image file. A specially-crafted .psd file can cause a read of arbitrary memory address which can lead to denial of service. An attacker can provide a	N/A	A-OPE-OPEN-090123/485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious file to trigger this vulnerability. **CVE ID : CVE-2022-41684**		
Vendor: openimageio_project					
Product: openimageio					
Affected Version(s): 2.3.19.0					
Write-what-where Condition	22-Dec-2022	9.8	A heap out-of-bounds write vulnerability exists in the way OpenImageIO v2.3.19.0 processes RLE encoded BMP images. A specially-crafted bmp file can write to arbitrary out of bounds memory, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-38143**	N/A	A-OPE-OPEN-090123/486
Heap-based Buffer Overflow	22-Dec-2022	9.8	A heap based buffer overflow vulnerability exists in tile decoding code of TIFF image parser in OpenImageIO master-branch-9aeece7a and v2.3.19.0. A specially-crafted TIFF file can lead to an out of bounds memory corruption, which can result in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	N/A	A-OPE-OPEN-090123/487

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41639		
Heap-based Buffer Overflow	22-Dec-2022	9.8	A heap based buffer overflow vulnerability exists in the PSD thumbnail resource parsing code of OpenImageIO 2.3.19.0. A specially-crafted PSD file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-41794**	N/A	A-OPE-OPEN-090123/488
Out-of-bounds Read	22-Dec-2022	9.1	A heap out of bounds read vulnerability exists in the handling of IPTC data while parsing TIFF images in OpenImageIO v2.3.19.0. A specially-crafted TIFF file can cause a read of adjacent heap memory, which can leak sensitive process information. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-41649**	N/A	A-OPE-OPEN-090123/489
Stack-based Buffer Overflow	22-Dec-2022	8.1	A stack-based buffer overflow vulnerability exists in the TGA file format parser of OpenImageIO v2.3.19.0. A specially-crafted targa file can lead to out of bounds read and write on the process stack, which can lead to	N/A	A-OPE-OPEN-090123/490

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-41981**		
Out-of-bounds Read	22-Dec-2022	7.5	An information disclosure vulnerability exists in the OpenImageIO::decode_iptc_iim() functionality of OpenImageIO Project OpenImageIO v2.3.19.0. A specially-crafted TIFF file can lead to a disclosure of sensitive information. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-41988**	N/A	A-OPE-OPEN-090123/491
NULL Pointer Dereference	22-Dec-2022	7.5	A denial of service vulnerability exists in the DDS native tile reading functionality of OpenImageIO Project OpenImageIO v2.3.19.0 and v2.4.4.2. A specially-crafted .dds can lead to denial of service. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-41999**	N/A	A-OPE-OPEN-090123/492
Off-by-one Error	22-Dec-2022	5.3	A heap out-of-bounds read vulnerability exists in the RLA format parser of OpenImageIO	N/A	A-OPE-OPEN-090123/493

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			master-branch-9aeece7a and v2.3.19.0. More specifically, in the way run-length encoded byte spans are handled. A malformed RLA file can lead to an out-of-bounds read of heap metadata which can result in sensitive information leak. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-36354**		
Affected Version(s): 2.4.4.2					
Out-of-bounds Write	22-Dec-2022	9.8	An out-of-bounds write vulnerability exists in the OpenImageIO::add_exif_item_to_spec functionality of OpenImageIO Project OpenImageIO v2.4.4.2. Specially-crafted exif metadata can lead to stack-based memory corruption. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-41837**	N/A	A-OPE-OPEN-090123/494
Heap-based Buffer Overflow	22-Dec-2022	9.8	A code execution vulnerability exists in the DDS scanline parsing functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially-crafted .dds can lead to a heap	N/A	A-OPE-OPEN-090123/495

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			buffer overflow. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-41838**		
Heap-based Buffer Overflow	22-Dec-2022	8.1	Multiple memory corruption vulnerabilities exist in the IFFOutput alignment padding functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to arbitrary code execution. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises when the `m_spec.format` is `TypeDesc::UINT8`. **CVE ID : CVE-2022-43597**	N/A	A-OPE-OPEN-090123/496
Heap-based Buffer Overflow	22-Dec-2022	8.1	Multiple memory corruption vulnerabilities exist in the IFFOutput alignment padding functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to arbitrary code execution. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises	N/A	A-OPE-OPEN-090123/497

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			when the `m_spec.format` is `TypeDesc::UINT16`. **CVE ID : CVE-2022-43598**		
Heap-based Buffer Overflow	22-Dec-2022	8.1	Multiple code execution vulnerabilities exist in the IFFOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to a heap buffer overflow. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises when the `xmax` variable is set to 0xFFFF and `m_spec.format` is `TypeDesc::UINT8` **CVE ID : CVE-2022-43599**	N/A	A-OPE-OPEN-090123/498
Heap-based Buffer Overflow	22-Dec-2022	8.1	Multiple code execution vulnerabilities exist in the IFFOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to a heap buffer overflow. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises when the `xmax` variable is set to 0xFFFF and	N/A	A-OPE-OPEN-090123/499

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`m_spec.format` is `TypeDesc::UINT16` **CVE ID : CVE-2022-43600**		
Heap-based Buffer Overflow	22-Dec-2022	8.1	Multiple code execution vulnerabilities exist in the IFFOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to a heap buffer overflow. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises when the `ymax` variable is set to 0xFFFF and `m_spec.format` is `TypeDesc::UINT16` **CVE ID : CVE-2022-43601**	N/A	A-OPE-OPEN-090123/500
Heap-based Buffer Overflow	22-Dec-2022	8.1	Multiple code execution vulnerabilities exist in the IFFOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to a heap buffer overflow. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises when the `ymax` variable is set to 0xFFFF and	N/A	A-OPE-OPEN-090123/501

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			`m_spec.format` is `TypeDesc::UINT8` **CVE ID : CVE-2022-43602**		
NULL Pointer Dereference	22-Dec-2022	7.5	A denial of service vulnerability exists in the DDS native tile reading functionality of OpenImageIO Project OpenImageIO v2.3.19.0 and v2.4.4.2. A specially-crafted .dds can lead to denial of service. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-41999**	N/A	A-OPE-OPEN-090123/502
Out-of-bounds Read	22-Dec-2022	5.9	An information disclosure vulnerability exists in the DPXOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to leaked heap data. An attacker can provide malicious input to trigger this vulnerability. **CVE ID : CVE-2022-43592**	N/A	A-OPE-OPEN-090123/503
NULL Pointer Dereference	22-Dec-2022	5.9	A denial of service vulnerability exists in the DPXOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted	N/A	A-OPE-OPEN-090123/504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ImageOutput Object can lead to null pointer dereference. An attacker can provide malicious input to trigger this vulnerability. **CVE ID : CVE-2022-43593**		
NULL Pointer Dereference	22-Dec-2022	5.9	Multiple denial of service vulnerabilities exist in the image output closing functionality of OpenImageIO Project OpenImageIO v2.4.4.2. Specially crafted ImageOutput Objects can lead to multiple null pointer dereferences. An attacker can provide malicious multiple inputs to trigger these vulnerabilities.This vulnerability applies to writing .bmp files. **CVE ID : CVE-2022-43594**	N/A	A-OPE-OPEN-090123/505
NULL Pointer Dereference	22-Dec-2022	5.9	Multiple denial of service vulnerabilities exist in the image output closing functionality of OpenImageIO Project OpenImageIO v2.4.4.2. Specially crafted ImageOutput Objects can lead to multiple null pointer dereferences. An attacker can provide malicious multiple inputs to trigger these vulnerabilities.This	N/A	A-OPE-OPEN-090123/506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability applies to writing .fits files. **CVE ID : CVE-2022-43595**		
Out-of-bounds Read	22-Dec-2022	5.9	An information disclosure vulnerability exists in the IFFOutput channel interleaving functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to leaked heap data. An attacker can provide malicious input to trigger this vulnerability. **CVE ID : CVE-2022-43596**	N/A	A-OPE-OPEN-090123/507
NULL Pointer Dereference	22-Dec-2022	5.9	A denial of service vulnerability exists in the ZfileOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to denial of service. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2022-43603**	N/A	A-OPE-OPEN-090123/508
Vendor: Openstack					
Product: kolla					
Affected Version(s): -					
Improper Privilege	21-Dec-2022	7.8	A privilege escalation vulnerability exists in the sudo functionality	N/A	A-OPE-KOLL-090123/509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Management			of OpenStack Kolla git master 05194e7618. A misconfiguration in /etc/sudoers within a container can lead to increased privileges. **CVE ID : CVE-2022-38060**		
Vendor: Otrs					
Product: otrs					
Affected Version(s): 7.0.40					
Improper Input Validation	19-Dec-2022	9.8	Improper Input Validation vulnerability in OTRS AG OTRS, OTRS AG ((OTRS)) Community Edition allows SQL Injection via TicketSearch Webservice This issue affects OTRS: from 7.0.1 before 7.0.40 Patch 1, from 8.0.1 before 8.0.28 Patch 1; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34. **CVE ID : CVE-2022-4427**	https://otrs.com/release-notes/otrs-security-advisory-2022-15/	A-OTR-OTRS-090123/510
Affected Version(s): 8.0.28					
Improper Input Validation	19-Dec-2022	9.8	Improper Input Validation vulnerability in OTRS AG OTRS, OTRS AG ((OTRS)) Community Edition allows SQL Injection via TicketSearch Webservice This issue affects OTRS: from 7.0.1 before 7.0.40 Patch 1, from 8.0.1 before 8.0.28 Patch 1; ((OTRS))	https://otrs.com/release-notes/otrs-security-advisory-2022-15/	A-OTR-OTRS-090123/511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Community Edition: from 6.0.1 through 6.0.34. **CVE ID : CVE-2022-4427**		
Affected Version(s): From (including) 6.0.1 Up to (including) 6.0.34					
Improper Input Validation	19-Dec-2022	9.8	Improper Input Validation vulnerability in OTRS AG OTRS, OTRS AG ((OTRS)) Community Edition allows SQL Injection via TicketSearch Webservice This issue affects OTRS: from 7.0.1 before 7.0.40 Patch 1, from 8.0.1 before 8.0.28 Patch 1; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34. **CVE ID : CVE-2022-4427**	https://otrs.com/release-notes/otrs-security-advisory-2022-15/	A-OTR-OTRS-090123/512
Affected Version(s): From (including) 7.0.1 Up to (excluding) 7.0.40					
Improper Input Validation	19-Dec-2022	9.8	Improper Input Validation vulnerability in OTRS AG OTRS, OTRS AG ((OTRS)) Community Edition allows SQL Injection via TicketSearch Webservice This issue affects OTRS: from 7.0.1 before 7.0.40 Patch 1, from 8.0.1 before 8.0.28 Patch 1; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34. **CVE ID : CVE-2022-4427**	https://otrs.com/release-notes/otrs-security-advisory-2022-15/	A-OTR-OTRS-090123/513

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 8.0.1 Up to (excluding) 8.0.28					
Improper Input Validation	19-Dec-2022	9.8	Improper Input Validation vulnerability in OTRS AG OTRS, OTRS AG ((OTRS)) Community Edition allows SQL Injection via TicketSearch Webservice This issue affects OTRS: from 7.0.1 before 7.0.40 Patch 1, from 8.0.1 before 8.0.28 Patch 1; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34. **CVE ID : CVE-2022-4427**	https://otrs.com/release-notes/otrs-security-advisory-2022-15/	A-OTR-OTRS-090123/514
Vendor: p4_project					
Product: p4					
Affected Version(s): * Up to (excluding) 0.0.7					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Dec-2022	9.8	The package p4 before 0.0.7 are vulnerable to Command Injection via the run() function due to improper input sanitization **CVE ID : CVE-2022-25171**	https://security.snyk.io/vuln/SNYK-JS-P4-3167330, https://github.com/natelong/p4/blob/master/p4.js%23L12, https://github.com/natelong/p4/commit/ae42e251beabf67c00539ec0e1d7aa149ca445fb	A-P4_-P4-090123/515
Vendor: patchelf_project					
Product: patchelf					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 0.9					
Out-of-bounds Read	19-Dec-2022	9.1	Patchelf v0.9 was discovered to contain an out-of-bounds read via the function modifyRPath at src/patchelf.cc. **CVE ID : CVE-2022-44940**	https://github.com/NixOS/patchelf/pull/419	A-PAT-PATC-090123/516
Vendor: pdftojson_project					
Product: pdftojson					
Affected Version(s): -					
Out-of-bounds Write	19-Dec-2022	9.8	pdftojson commit 94204bb was discovered to contain a stack overflow via the component Object::copy(Object*):Object.cc. **CVE ID : CVE-2022-44108**	N/A	A-PDF-PDFT-090123/517
Affected Version(s): * Up to (excluding) 2017-10-28					
Out-of-bounds Write	19-Dec-2022	9.8	pdftojson commit 94204bb was discovered to contain a stack overflow via the component Stream::makeFilter(char*, Stream*, Object*, int). **CVE ID : CVE-2022-44109**	N/A	A-PDF-PDFT-090123/518
Vendor: Pfsense					
Product: pfblockerng					
Affected Version(s): * Up to (excluding) 2.1.4_27					
Improper Neutralization of Special	20-Dec-2022	9.8	pfSense pfBlockerNG through 2.1.4_27 allows remote attackers to execute arbitrary OS	https://docs.netgate.com/pfsense/en/latest/pack	A-PFS-PFBL-090123/519

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			commands as root via the HTTP Host header, a different vulnerability than CVE-2022-31814. **CVE ID : CVE-2022-40624**	ages/pfblocker.html	
Vendor: pi-hole					
Product: adminlte					
Affected Version(s): * Up to (including) 5.17					
Improper Access Control	23-Dec-2022	5.3	Pi-Hole is a network-wide ad blocking via your own Linux hardware, AdminLTE is a Pi-hole Dashboard for stats and more. In case of an attack, the threat actor will obtain the ability to perform an unauthorized query for blocked domains on `queryads` endpoint. In the case of application, this vulnerability exists because of a lack of validation in code on a root server path: `/admin/scripts/pi-hole/phpqueryads.php.` Potential threat actor(s) are able to perform an unauthorized query search in blocked domain lists. This could lead to the disclosure for any victims' personal blacklists. **CVE ID : CVE-2022-23513**	N/A	A-PI--ADMI-090123/520
Vendor: pig-vector_project					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: pig-vector					
Affected Version(s): -					
Insecure Temporary File	21-Dec-2022	5.5	A vulnerability was found in pig-vector and classified as problematic. Affected by this issue is the function LogisticRegression of the file src/main/java/org/apache/mahout/pig/LogisticRegression.java. The manipulation leads to insecure temporary file. The attack needs to be approached locally. The name of the patch is 1e7bd9fab5401a2df18d2eabd802adcf0dcf1f15. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216500. **CVE ID : CVE-2022-4641**	https://github.com/tdunning/pig-vector/pull/2, https://github.com/tdunning/pig-vector/commit/1e7bd9fab5401a2df18d2eabd802adcf0dcf1f15	A-PIG-PIG--090123/521
Vendor: pivotal_software					
Product: concourse					
Affected Version(s): From (including) 6.0.0 Up to (excluding) 6.7.9					
Incorrect Authorization	19-Dec-2022	5.4	Concourse (7.x.y prior to 7.8.3 and 6.x.y prior to 6.7.9) contains an authorization bypass issue. A Concourse user can send a request with body including :team_name=team2 to bypass team scope check to gain access to certain resources	N/A	A-PIV-CONC-090123/522

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			belong to any other team. **CVE ID : CVE-2022-31683**		
Affected Version(s): From (including) 7.0.0 Up to (excluding) 7.8.3					
Incorrect Authorization	19-Dec-2022	5.4	Concourse (7.x.y prior to 7.8.3 and 6.x.y prior to 6.7.9) contains an authorization bypass issue. A Concourse user can send a request with body including :team_name=team2 to bypass team scope check to gain access to certain resources belong to any other team. **CVE ID : CVE-2022-31683**	N/A	A-PIV-CONC-090123/523
Vendor: pluginus					
Product: inpost_gallery					
Affected Version(s): * Up to (excluding) 2.1.4.1					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Dec-2022	9.8	The InPost Gallery WordPress plugin before 2.1.4.1 insecurely uses PHP's extract() function when rendering HTML views, allowing attackers to force the inclusion of malicious files & URLs, which may enable them to run code on servers. **CVE ID : CVE-2022-4063**	N/A	A-PLU-INPO-090123/524
Vendor: popup_manager_project					
Product: popup_manager					
Affected Version(s): * Up to (including) 1.6.6					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	19-Dec-2022	4.3	The Popup Manager WordPress plugin through 1.6.6 does not have authorisation and CSRF checks when deleting popups, which could allow unauthenticated users to delete them **CVE ID : CVE-2022-4124**	N/A	A-POP-POPU-090123/525
Cross-Site Request Forgery (CSRF)	19-Dec-2022	4.3	The Popup Manager WordPress plugin through 1.6.6 does not have authorisation and CSRF check when creating/updating popups, and is missing sanitisation as well as escaping, which could allow unauthenticated attackers to create arbitrary popups and add Stored XSS payloads as well **CVE ID : CVE-2022-4125**	N/A	A-POP-POPU-090123/526
Vendor: Poweriso					
Product: poweriso					
Affected Version(s): 8.3					
Out-of-bounds Write	16-Dec-2022	7.8	A memory corruption vulnerability exists in the VHD File Format parsing CXSPARSE record functionality of PowerISO PowerISO 8.3. A specially-crafted file can lead to an out-of-bounds write. A victim needs to open a	N/A	A-POW-POWE-090123/527

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malicious file to trigger this vulnerability. **CVE ID : CVE-2022-41992**		
Vendor: properfraction					
Product: profilepress					
Affected Version(s): * Up to (excluding) 4.5.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Dec-2022	4.8	The ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wp_user_cover_default_image_url' parameter in versions up to, and including, 4.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2022-4697**	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&new=2838522%40wp-user-avatar%2Ftrunk&old=2837217%40wp-user-avatar%2Ftrunk&sfp_email=&sfph_mail=	A-PRO-PROF-090123/528
Improper Neutralization of Input During Web Page Generation	23-Dec-2022	4.8	The ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several form fields in versions up to, and including, 4.5.0 due to	https://plugins.trac.wordpress.org/changeset?sfp_email=&sfph_mail=&reponame=&ne	A-PRO-PROF-090123/529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. **CVE ID : CVE-2022-4698**	w=2838522%40wp-user-avatar%2Ftrunk&old=2837217%40wp-user-avatar%2Ftrunk&sfp_email=&sfph_mail=	
Vendor: Python					
Product: setuptools					
Affected Version(s): * Up to (excluding) 65.5.1					
N/A	23-Dec-2022	7.5	Python Packaging Authority (PyPA) setuptools before 65.5.1 allows remote attackers to cause a denial of service via HTML in a crafted package or custom PackageIndex page. There is a Regular Expression Denial of Service (ReDoS) in package_index.py. **CVE ID : CVE-2022-40897**	https://pyup.io/posts/pyup-discovers-redos-vulnerabilities-in-top-python-packages/, https://github.com/pypa/setuptools/compare/v65.5.0...v65.5.1, https://github.com/pypa/setuptools/commit/43a9c9bfa6aa6	A-PYT-SETU-090123/530

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				26ec2a22540bea28d2ca77964be	
Vendor: pythoncharmers					
Product: python-future					
Affected Version(s): * Up to (including) 0.18.2					
N/A	23-Dec-2022	7.5	An issue discovered in Python Charmers Future 0.18.2 and earlier allows remote attackers to cause a denial of service via crafted Set-Cookie header from malicious web server. **CVE ID : CVE-2022-40899**	https://github.com/python/cpython/pull/17157, https://pyup.io/posts/pyup-discovers-redos-vulnerabilities-in-top-python-packages/	A-PYT-PYTH-090123/531
Vendor: Redhat					
Product: openstack					
Affected Version(s): -					
Incorrect Permission Assignment for Critical Resource	21-Dec-2022	8.8	A privilege escalation vulnerability exists in the oslo.privsep functionality of OpenStack git master 05194e7618 and prior. Overly permissive functionality within tools leveraging this library within a container can lead increased privileges. **CVE ID : CVE-2022-38065**	N/A	A-RED-OPEN-090123/532
Product: satellite					
Affected Version(s): 6.10					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Dec-2022	7.5	A blind site-to-site request forgery vulnerability was found in Satellite server. It is possible to trigger an external interaction to an attacker's server by modifying the Referer header in an HTTP request of specific resources in the server. **CVE ID : CVE-2022-4130**	https://bugzilla.redhat.com/show_bug.cgi?id=2145254	A-RED-SATE-090123/533
Affected Version(s): 6.11					
N/A	16-Dec-2022	7.5	A blind site-to-site request forgery vulnerability was found in Satellite server. It is possible to trigger an external interaction to an attacker's server by modifying the Referer header in an HTTP request of specific resources in the server. **CVE ID : CVE-2022-4130**	https://bugzilla.redhat.com/show_bug.cgi?id=2145254	A-RED-SATE-090123/534
Affected Version(s): 6.9					
N/A	16-Dec-2022	7.5	A blind site-to-site request forgery vulnerability was found in Satellite server. It is possible to trigger an external interaction to an attacker's server by modifying the Referer header in an HTTP request of specific resources in the server. **CVE ID : CVE-2022-4130**	https://bugzilla.redhat.com/show_bug.cgi?id=2145254	A-RED-SATE-090123/535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: retra-system_project					
Product: retra-system					
Affected Version(s): * Up to (excluding) 2022-01-07					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2022	6.1	A vulnerability was found in retra-system. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is a6d94ab88f4a6f631a14c59b72461140fb57ae1f. It is recommended to apply a patch to fix this issue. VDB-216186 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4593**	https://github.com/retra/retra-system/commit/a6d94ab88f4a6f631a14c59b72461140fb57ae1f	A-RET-RETR-090123/536
Vendor: rockoa					
Product: xinhu					
Affected Version(s): * Up to (excluding) 2.5.0					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-Dec-2022	7.5	SQL Injection exits in xinhu < 2.5.0 **CVE ID : CVE-2022-45041**	N/A	A-ROC-XINH-090123/537
Vendor: ruoyi_project					
Product: ruoyi					
Affected Version(s): 4.7.5					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Dec-2022	9.8	A vulnerability, which was classified as critical, has been found in y_project RuoYi 4.7.5. This issue affects some unknown processing of the file com/ruoyi/generator/controller/GenController. The manipulation leads to sql injection. The name of the patch is 167970e5c4da7bb46217f576dc50622b83f32b40. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-215975. **CVE ID : CVE-2022-4566**	N/A	A-RUO-RUOY-090123/538
Vendor: safe-eval_project					
Product: safe-eval					
Affected Version(s): * Up to (including) 0.4.1					
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	20-Dec-2022	9.8	All versions of package safe-eval are vulnerable to Prototype Pollution which allows an attacker to add or modify properties of the Object.prototype.Consolidate when using the function safeEval. This is because the function uses vm variable, leading an attacker to modify properties of the Object.prototype.	https://github.com/hacksparrow/safe-eval/issues/26, https://security.snyk.io/vuln/SNYK-JS-SAFEEVAL-3175701	A-SAF-SAFE-090123/539

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-25904		
Vendor: Samba					
Product: ppp					
Affected Version(s): * Up to (excluding) 2022-08-03					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-Dec-2022	8.8	** DISPUTED ** A vulnerability classified as problematic has been found in ppp. Affected is the function dumpppp of the file pppdump/pppdump.c of the component pppdump. The manipulation of the argument spkt.buf/rpkt.buf leads to improper validation of array index. The real existence of this vulnerability is still doubted at the moment. The name of the patch is a75fb7b198eed50d769c80c36629f38346882cbf. It is recommended to apply a patch to fix this issue. VDB-216198 is the identifier assigned to this vulnerability. NOTE: pppdump is not used in normal process of setting up a PPP connection, is not installed setuid-root, and is not invoked automatically in any scenario. **CVE ID : CVE-2022-4603**	https://github.com/ppp-project/ppp/commit/a75fb7b198eed50d769c80c36629f38346882cbf	A-SAM-PPP-090123/540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: search					
Product: docconv					
Affected Version(s): * Up to (excluding) 1.2.1					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	A vulnerability was found in docconv up to 1.2.0. It has been declared as critical. This vulnerability affects the function ConvertPDFImages of the file pdf_ocr.go. The manipulation of the argument path leads to os command injection. The attack can be initiated remotely. Upgrading to version 1.2.1 is able to address this issue. The name of the patch is b19021ade3d0b71c89d35cb00eb9e589a121faa5. It is recommended to upgrade the affected component. VDB-216502 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4643**	https://github.com/sajari/docconv/pull/110, https://github.com/sajari/docconv/commit/b19021ade3d0b71c89d35cb00eb9e589a121faa5, https://github.com/sajari/docconv/releases/tag/v1.2.1	A-SEA-DOCC-090123/541
Vendor: shoplazza					
Product: lifestyle					
Affected Version(s): 1.1					
Improper Neutralization of Input During Web Page Generation	18-Dec-2022	5.4	A vulnerability, which was classified as problematic, has been found in Shoplazza 1.1. This issue affects some unknown processing of the file /admin/api/admin/arti	N/A	A-SHO-LIFE-090123/542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			cles/ of the component Add Blog Post Handler. The manipulation of the argument Title leads to cross site scripting. 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-216191. **CVE ID : CVE-2022-4596**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2022	5.4	A vulnerability, which was classified as problematic, was found in Shoplazza LifeStyle 1.1. Affected is an unknown function of the file /admin/api/admin/v2_products of the component Create Product Handler. The manipulation 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-216192. **CVE ID : CVE-2022-4597**	N/A	A-SHO-LIFE-090123/543
Improper Neutralization of Input During	18-Dec-2022	5.4	A vulnerability has been found in Shoplazza LifeStyle 1.1 and classified as problematic. Affected	N/A	A-SHO-LIFE-090123/544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			by this vulnerability is an unknown functionality of the file /admin/api/theme-edit/ of the component Announcement Handler. The manipulation of the argument Text/Mobile Text leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-216193 was assigned to this vulnerability. **CVE ID : CVE-2022-4598**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2022	5.4	A vulnerability was found in Shoplazza LifeStyle 1.1 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/api/theme-edit/ of the component Product Handler. The manipulation of the argument Subheading/Heading/Text/Button Text/Label leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-216194 is	N/A	A-SHO-LIFE-090123/545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4599**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2022	5.4	A vulnerability was found in Shoplazza LifeStyle 1.1. It has been classified as problematic. This affects an unknown part of the file /admin/api/theme-edit/ of the component Product Carousel Handler. The manipulation of the argument Heading/Description leads to cross site scripting. 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-216195. **CVE ID : CVE-2022-4600**	N/A	A-SHO-LIFE-090123/546
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2022	5.4	A vulnerability was found in Shoplazza LifeStyle 1.1. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/api/theme-edit/ of the component Shipping/Member Discount/Icon. The manipulation leads to cross site scripting. The	N/A	A-SHO-LIFE-090123/547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-216196. **CVE ID : CVE-2022-4601**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Dec-2022	5.4	A vulnerability was found in Shoplazza LifeStyle 1.1. It has been rated as problematic. This issue affects some unknown processing of the file /admin/api/theme-edit/ of the component Review Flow Handler. The manipulation of the argument Title leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-216197 was assigned to this vulnerability. **CVE ID : CVE-2022-4602**	N/A	A-SHO-LIFE-090123/548
Vendor: silverwaregames					
Product: silverwaregames					
Affected Version(s): * Up to (excluding) 1.1.34					
Improper Neutralization of Input During Web Page Generation	19-Dec-2022	5.4	Silverware Games is a social network where people can play games online. Users can attach URLs to YouTube videos, the site will generate related	N/A	A-SIL-SILV-090123/549

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			`<iframe>` when the post will be published. The handler has some sort of protection so non-YouTube links can't be posted, as well as HTML tags are being stripped. However, it was still possible to add custom HTML attributes (e.g. `onclick=alert("xss")`) to the `<iframe>'. This issue was fixed in the version `1.1.34` and does not require any extra actions from our members. There has been no evidence that this vulnerability was used by anyone at this time. **CVE ID : CVE-2022-23543**		
Vendor: simmeth					
Product: lieferantenmanager					
Affected Version(s): * Up to (excluding) 5.6					
Improper Authentication	25-Dec-2022	9.1	An issue was discovered in Simmeth Lieferantenmanager before 5.6. An attacker can make various API calls without authentication because the password in a Credential Object is not checked. **CVE ID : CVE-2022-44013**	N/A	A-SIM-LIEF-090123/550
Improper Limitation of a	25-Dec-2022	7.5	An issue was discovered in Simmeth Lieferantenmanager	N/A	A-SIM-LIEF-090123/551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			before 5.6. An attacker can download arbitrary files from the web server by abusing an API call: /DS/LM_API/api/ConfigurationService/GetImages with an '"ImagesPath":"C:\\"' value. **CVE ID : CVE-2022-44016**		
N/A	25-Dec-2022	6.5	An issue was discovered in Simmeth Lieferantenmanager before 5.6. In the design of the API, a user is inherently able to fetch arbitrary SQL tables. This leaks all user passwords and MSSQL hashes via /DS/LM_API/api/SelectionService/GetPaggedTab. **CVE ID : CVE-2022-44014**	N/A	A-SIM-LIEF-090123/552
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Dec-2022	5.4	An issue was discovered in /DS/LM_API/api/SelectionService/InsertQueryWithActiveRelationsReturnId in Simmeth Lieferantenmanager before 5.6. An attacker can execute JavaScript code in the browser of the victim if a site is loaded. The victim's encrypted password can be stolen and most likely be decrypted.	N/A	A-SIM-LIEF-090123/553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-44012		
Vendor: smoothiecharts					
Product: smoothie_charts					
Affected Version(s): From (including) 1.31.0 Up to (excluding) 1.36.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2022	5.4	The package smoothie from 1.31.0 and before 1.36.1 are vulnerable to Cross-site Scripting (XSS) due to improper user input sanitization in strokeStyle and tooltipLabel properties. Exploiting this vulnerability is possible when the user can control these properties. **CVE ID : CVE-2022-25929**	https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-3177369, https://github.com/joewalnes/smoothie/pull/147, https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-3177368, https://security.snyk.io/vuln/SNYK-JS-SMOOTHIE-3177364	A-SMO-SMOO-090123/554
Vendor: snipeitapp					
Product: snipe-it					
Affected Version(s): * Up to (excluding) 6.0.14					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-Dec-2022	5.4	Snipe-IT before 6.0.14 is vulnerable to Cross Site Scripting (XSS) for View Assigned Assets. **CVE ID : CVE-2022-44380**	https://census-labs.com/news/2022/12/23/multiple-vulnerabilities-in-snipe-it/	A-SNI-SNIP-090123/555

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 6.0.14					
Observable Discrepancy	25-Dec-2022	5.3	Snipe-IT through 6.0.14 allows attackers to check whether a user account exists because of response variations in a /password/reset request. **CVE ID : CVE-2022-44381**	https://census-labs.com/news/2022/12/23/multiple-vulnerabilities-in-snipe-it/	A-SNI-SNIP-090123/556
Vendor: softr					
Product: softr					
Affected Version(s): 2.0					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-Dec-2022	9.8	Softr v2.0 was discovered to be vulnerable to HTML injection via the Name field of the Account page. **CVE ID : CVE-2022-40434**	N/A	A-SOF-SOFT-090123/557
Vendor: Solarwinds					
Product: serv-u					
Affected Version(s): 15.3.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	5.4	This vulnerability happens in the web client versions 15.3.0 to Serv-U 15.3.1. This vulnerability affects the directory creation function. **CVE ID : CVE-2022-38106**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-38106, https://documentation.solarwinds.co	A-SOL-SERV-090123/558

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				m/en/success_center/servu/content/release_notes/servu_15-3-2_release_notes.htm	
Affected Version(s): 15.3.1					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	5.4	This vulnerability happens in the web client versions 15.3.0 to Serv-U 15.3.1. This vulnerability affects the directory creation function. **CVE ID : CVE-2022-38106**	https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-38106, https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_15-3-2_release_notes.htm	A-SOL-SERV-090123/559
Product: solarwinds_platform					
Affected Version(s): 2022.4.0					
Cleartext Storage of Sensitive Information	19-Dec-2022	5.5	Sensitive information was stored in plain text in a file that is accessible by a user with a local account in Hybrid Cloud Observability (HCO)/ SolarWinds Platform 2022.4. No other versions are affected **CVE ID : CVE-2022-47512**	https://documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/solarwinds_platform_2022-4-1_release_no	A-SOL-SOLA-090123/560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				tes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-47512	
Vendor: sslh_project					
Product: sslh					
Affected Version(s): 2.0					
Use of Externally-Controlled Format String	21-Dec-2022	9.8	A vulnerability, which was classified as critical, has been found in sslh. This issue affects the function hexdump of the file probe.c of the component Packet Dumping Handler. The manipulation of the argument msg_info leads to format string. The attack may be initiated remotely. The name of the patch is b19f8a6046b080e4c2e28354a58556bb26040c6f. It is recommended to apply a patch to fix this issue. The identifier VDB-216497 was assigned to this vulnerability. **CVE ID : CVE-2022-4639**	https://github.com/yrutschle/sslh/pull/353, https://github.com/yrutschle/sslh/commit/b19f8a6046b080e4c2e28354a58556bb26040c6f	A-SSL-SSLH-090123/561
Vendor: starter-public-edition-4_project					
Product: starter-public-edition-4					
Affected Version(s): * Up to (excluding) 4.6.11					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-2022	6.1	A vulnerability was found in starter-public-edition-4 up to 4.6.10. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 4.6.11 is able to address this issue. The name of the patch is 2606983c20f6ea3430ac4b36b3d2e88aafef45da. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216168. **CVE ID : CVE-2022-4582**	https://github.com/ivantcholakov/starter-public-edition-4/commit/2606983c20f6ea3430ac4b36b3d2e88aafef45da	A-STA-STAR-090123/562
Vendor: tatoeba					
Product: tatoeba2					
Affected Version(s): * Up to (excluding) 2022-10-30					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2022	5.4	A vulnerability was found in tatoeba2. It has been classified as problematic. This affects an unknown part of the component Profile Name Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version	https://github.com/Tatoeba/tatoeba2/issues/3002, https://github.com/Tatoeba/tatoeba2/commit/91110777fc8ddf1b4a2cf4e66e67db69b9700361	A-TAT-TATO-090123/563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			prod_2022-10-30 is able to address this issue. The name of the patch is 91110777fc8ddf1b4a2cf4e66e67db69b9700361. It is recommended to upgrade the affected component. The identifier VDB-216501 was assigned to this vulnerability. **CVE ID : CVE-2022-4642**		
Vendor: teluu					
Product: pjsip					
Affected Version(s): * Up to (excluding) 2.13.1					
Out-of-bounds Write	20-Dec-2022	9.8	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. Buffer overread is possible when parsing a specially crafted STUN message with unknown attribute. The vulnerability affects applications that uses STUN including PJNATH and PJSUA-LIB. The patch is available as a commit in the master branch (2.13.1). **CVE ID : CVE-2022-23537**	https://github.com/pjsip/pjproject/security/advisories/GHSA-9pfh-r8x4-w26w, https://github.com/pjsip/pjproject/commit/d8440f4d711a654b511f50f79c0445b26f9dd1e1	A-TEL-PJSI-090123/564
Vendor: thinkphp					
Product: thinkphp					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 6.0.14					
N/A	23-Dec-2022	9.8	ThinkPHP Framework before 6.0.14 allows local file inclusion via the lang parameter when the language pack feature is enabled (lang_switch_on=true). An unauthenticated and remote attacker can exploit this to execute arbitrary operating system commands, as demonstrated by including pearcmd.php. **CVE ID : CVE-2022-47945**	https://github.com/top-think/framework/compare/v6.0.13...v6.0.14, https://github.com/top-think/framework/commit/c4acb8b4001b98a0078eda25840d33e295a7f099	A-THI-THIN-090123/565
Vendor: tjws2_project					
Product: tjws2					
Affected Version(s): * Up to (excluding) 2022-05-24					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Dec-2022	9.8	A vulnerability was found in drogatkin TJWS2. It has been declared as critical. Affected by this vulnerability is the function deployWar of the file 1.x/src/rogatkin/web/WarRoller.java. The manipulation leads to path traversal. The attack can be launched remotely. The name of the patch is 1bac15c496ec54efe21ad7fab4e17633778582fc. It is recommended to apply a patch to fix this issue. The associated identifier of this	https://github.com/drogatkin/TJWS2/commit/1bac15c496ec54efe21ad7fab4e17633778582fc	A-TJW-TJWS-090123/566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is VDB-216187. **CVE ID : CVE-2022-4594**		
Vendor: toto_project					
Product: toto					
Affected Version(s): * Up to (excluding) 1.4.21					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Dec-2022	6.1	A vulnerability was found in mschaef toto up to 1.4.20. It has been classified as problematic. This affects an unknown part of the component Todo List Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 1.4.21 is able to address this issue. The name of the patch is fdc825ac5249f40683377e8a526a06cdc6870125. It is recommended to upgrade the affected component. The identifier VDB-216177 was assigned to this vulnerability. **CVE ID : CVE-2022-4590**	https://github.com/mschaef/toto/commit/fdc825ac5249f40683377e8a526a06cdc6870125	A-TOT-TOTO-090123/567
Improper Neutralization of Input During Web Page Generation	17-Dec-2022	6.1	A vulnerability was found in mschaef toto up to 1.4.20. It has been declared as problematic. This vulnerability affects unknown code of the component Email Parameter Handler. The	https://github.com/mschaef/toto/commit/1f27f37c1a06f54a76971f70eaa6139dc139bdf9	A-TOT-TOTO-090123/568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			manipulation leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 1.4.21 is able to address this issue. The name of the patch is 1f27f37c1a06f54a76971f70eaa6139dc139bdf9. It is recommended to upgrade the affected component. VDB-216178 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4591**		
Vendor: trellix					
Product: endpoint_security					
Affected Version(s): * Up to (excluding) 35.31.22					
Improper Preservation of Permissions	16-Dec-2022	6	Improper preservation of permissions vulnerability in Trellix Endpoint Agent (xAgent) prior to V35.31.22 on Windows allows a local user with administrator privileges to bypass the product protection to uninstall the agent via incorrectly applied permissions in the removal protection functionality. **CVE ID : CVE-2022-4326**	https://docs.trellix.com/bundle/xagent_35-31-22_rn/page/UUID-73c848e7-6107-fe11-d83d-b17bd5b1449c.html	A-TRE-ENDP-090123/569
Vendor: tum					
Product: ogc_web_feature_service					
Affected Version(s): * Up to (excluding) 5.3.0					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference	18-Dec-2022	9.8	A vulnerability was found in 3D City Database OGC Web Feature Service up to 5.2.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to xml external entity reference. Upgrading to version 5.2.1 is able to address this issue. The name of the patch is 246f4e2a97ad81491c00a7ed72ce5e7c7f75050a. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216215. **CVE ID : CVE-2022-4607**	https://github.com/3dcitydb/web-feature-service/pull/12, https://github.com/3dcitydb/web-feature-service/commit/246f4e2a97ad81491c00a7ed72ce5e7c7f75050a	A-TUM-OGC_-090123/570
Vendor: typora					
Product: typora					
Affected Version(s): * Up to (including) 1.38					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Dec-2022	6.1	Cross Site Scripting (XSS) vulnerability in typora through 1.38 allows remote attackers to run arbitrary code via export from editor. **CVE ID : CVE-2022-40011**	N/A	A-TYP-TYPO-090123/571
Vendor: ubi_reader_project					
Product: ubi_reader					
Affected Version(s): * Up to (including) 0.8.0					
Improper Limitation	17-Dec-2022	7.1	A vulnerability, which was classified as	https://github.com/jrsp	A-UBI-UBI_-090123/572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			problematic, has been found in UBI Reader up to 0.8.0. Affected by this issue is the function ubireader_extract_files of the file ubireader/ubifs/output.py of the component UBIFS File Handler. The manipulation leads to path traversal. The attack may be launched remotely. Upgrading to version 0.8.5 is able to address this issue. The name of the patch is d5d68e6b1b9f7070c29df5f67fc060f579ae9139. It is recommended to upgrade the affected component. VDB-216146 is the identifier assigned to this vulnerability. **CVE ID : CVE-2022-4572**	ruitt/ubi_reader/commit/d5d68e6b1b9f7070c29df5f67fc060f579ae9139, https://github.com/jrspruitt/ubi_reader/pull/57	
Vendor: ucf					
Product: materia					
Affected Version(s): * Up to (including) 9.0.0					
Cross-Site Request Forgery (CSRF)	16-Dec-2022	8.8	A vulnerability classified as problematic has been found in University of Central Florida Materia up to 9.0.0. This affects the function before of the file fuel/app/classes/controller/api.php of the component API Controller. The manipulation leads to	https://github.com/ucfopen/Materia/commit/af259115d2e8f17068e61902151ee8a9dbac397b, https://github.com/ucfopen/Materia/pull/1371	A-UCF-MATE-090123/573

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cross-site request forgery. It is possible to initiate the attack remotely. Upgrading to version 9.0.1-alpha1 is able to address this issue. The name of the patch is af259115d2e8f17068e61902151ee8a9dbac397b. It is recommended to upgrade the affected component. The identifier VDB-215973 was assigned to this vulnerability. **CVE ID : CVE-2022-4564**		
Vendor: ultimatemember					
Product: jobboardwp					
Affected Version(s): * Up to (excluding) 1.2.2					
Unrestricted Upload of File with Dangerous Type	19-Dec-2022	7.5	The JobBoardWP WordPress plugin before 1.2.2 does not properly validate file names and types in its file upload functionalities, allowing unauthenticated users to upload arbitrary files such as PHP. **CVE ID : CVE-2022-4061**	N/A	A-ULT-JOBB-090123/574
Vendor: usememos					
Product: memos					
Affected Version(s): * Up to (excluding) 0.9.0					
Improper Authentication	23-Dec-2022	9.8	Improper Authentication in GitHub repository	https://github.com/usememos/memos/commit/dca35bde8	A-USE-MEMO-090123/575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			usememos/memos prior to 0.9.0. **CVE ID : CVE-2022-4686**	77aab6e64ef51b52e590b5d48f692f9, https://huntr.dev/bounties/caa0b22c-501f-44eb-af65-65c315cd1637	
Improper Access Control	23-Dec-2022	8.8	Improper Access Control in GitHub repository usememos/memos prior to 0.9.0. **CVE ID : CVE-2022-4684**	https://huntr.dev/bounties/b66f2bdd-8b41-456c-bf65-92302c2e03b5, https://github.com/usememos/memos/commit/dca35bde877aab6e64ef51b52e590b5d48f692f9	A-USE-MEMO-090123/576
Improper Authorization	23-Dec-2022	8.8	Improper Authorization in GitHub repository usememos/memos prior to 0.9.0. **CVE ID : CVE-2022-4688**	https://huntr.dev/bounties/23856e7e-94ff-4dee-97d0-0cd47e9b8ff6, https://github.com/usememos/memos/commit/dca35bde877aab6e64ef51b52e590b5d48f692f9	A-USE-MEMO-090123/577
Improper Access Control	23-Dec-2022	8.8	Improper Access Control in GitHub repository	https://huntr.dev/bounties/a78c432	A-USE-MEMO-090123/578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			usememos/memos prior to 0.9.0. **CVE ID : CVE-2022-4689**	6-6e7b-47fe-aa82-461e5c12a4e3, https://github.com/usememos/memos/commit/dca35bde877aab6e64ef51b52e590b5d48f692f9	
Improper Privilege Management	23-Dec-2022	8.1	Incorrect Use of Privileged APIs in GitHub repository usememos/memos prior to 0.9.0. **CVE ID : CVE-2022-4687**	https://huntr.dev/bounties/b908377f-a61b-432c-8e6a-c7498da69788, https://github.com/usememos/memos/commit/dca35bde877aab6e64ef51b52e590b5d48f692f9	A-USE-MEMO-090123/579
Cleartext Transmission of Sensitive Information	23-Dec-2022	6.5	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository usememos/memos prior to 0.9.0. **CVE ID : CVE-2022-4683**	https://huntr.dev/bounties/84973f6b-739a-4d7e-8757-fc58cbbaf6ef, https://github.com/usememos/memos/commit/7efa749c6628c75b19a912ca170529f5c293bb2e	A-USE-MEMO-090123/580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.0. **CVE ID : CVE-2022-4609**	https://github.com/usememos/memos/commit/726285e63467820f94cbf872abe71025a161c212, https://hunt r.dev/bounties/5b3115c5-776c-43d3-a7be-c8dc13ab81ce	A-USE-MEMO-090123/581
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Dec-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.0. **CVE ID : CVE-2022-4690**	https://hunt r.dev/bounties/7e1be91d-3b13-4300-8af2-9bd9665ec335, https://github.com/usememos/memos/commit/c07b4a57caa89905e54b800f4d8fb720bbf5bf82	A-USE-MEMO-090123/582
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Dec-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.0. **CVE ID : CVE-2022-4692**	https://hunt r.dev/bounties/9d1ed6ea-f7a0-4561-9325-a2babef99c74, https://github.com/usememos/memos/commit/c07b4a57c	A-USE-MEMO-090123/583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				aa89905e54b800f4d8fb720bbf5bf82	
Vendor: vms-studio					
Product: quizlord					
Affected Version(s): * Up to (including) 2.0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	4.8	The Quizlord WordPress plugin through 2.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup). **CVE ID : CVE-2022-4112**	N/A	A-VMS-QUIZ-090123/584
Vendor: Vmware					
Product: vrealize_operations					
Affected Version(s): 8.10.0					
N/A	16-Dec-2022	7.2	vRealize Operations (vROps) contains a privilege escalation vulnerability. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 7.2. **CVE ID : CVE-2022-31707**	https://www.vmware.com/security/advisories/VMSA-2022-0034.html	A-VMW-VREA-090123/585
Exposure of	16-Dec-2022	4.9	vRealize Operations (vROps) contains a	https://www.vmware.c	A-VMW-VREA-090123/586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			broken access control vulnerability. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 4.4. **CVE ID : CVE-2022-31708**	om/security/advisories/VMSA-2022-0034.html	
Affected Version(s): From (including) 8.6.0 Up to (excluding) 8.6.4.20823815					
N/A	16-Dec-2022	7.2	vRealize Operations (vROps) contains a privilege escalation vulnerability. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 7.2. **CVE ID : CVE-2022-31707**	https://www.vmware.com/security/advisories/VMSA-2022-0034.html	A-VMW-VREA-090123/587
Exposure of Resource to Wrong Sphere	16-Dec-2022	4.9	vRealize Operations (vROps) contains a broken access control vulnerability. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 4.4. **CVE ID : CVE-2022-31708**	https://www.vmware.com/security/advisories/VMSA-2022-0034.html	A-VMW-VREA-090123/588
Vendor: Wbce					
Product: wbce_cms					
Affected Version(s): 1.5.4					
Unrestricted Upload of File with	20-Dec-2022	9.8	WBCE CMS v1.5.4 can implement getshell by	N/A	A-WBC-WBCE-090123/589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			modifying the upload file type. **CVE ID : CVE-2022-46020**		
Vendor: wfs					
Product: heaven_burns_red					
Affected Version(s): * Up to (including) 2.5.0					
Improper Privilege Management	20-Dec-2022	7.8	wfshbr64.sys and wfshbr32.sys specially crafted IOCTL allows arbitrary user to perform local privilege escalation **CVE ID : CVE-2022-42046**	https://www.wfs.games/news/20221220_01.html, https://github.com/kkent030315/CVE-2022-42046	A-WFS-HEAV-090123/590
Vendor: wheel_project					
Product: wheel					
Affected Version(s): * Up to (excluding) 0.38.1					
N/A	23-Dec-2022	7.5	An issue discovered in Python Packaging Authority (PyPA) Wheel 0.37.1 and earlier allows remote attackers to cause a denial of service via attacker controlled input to wheel cli. **CVE ID : CVE-2022-40898**	https://pyup.io/posts/pyup-discovers-redos-vulnerabilities-in-top-python-packages/	A-WHE-WHEE-090123/591
Vendor: wp-ban_project					
Product: wp-ban					
Affected Version(s): -					
Improper Neutralization of Input During	21-Dec-2022	6.1	A vulnerability, which was classified as problematic, was found in WP-Ban. Affected is an unknown function of	https://github.com/lesterchan/wp-ban/commit/22b925449	A-WP--WP-B-090123/592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			the file ban-options.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is 22b925449c84faa9b7496abe4f8f5661cb5eb3bf. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216480. **CVE ID : CVE-2022-4631**	c84faa9b7496abe4f8f5661cb5eb3bf	
Vendor: wp-english-wp-admin_project					
Product: wp-english-wp-admin					
Affected Version(s): * Up to (excluding) 1.5.3					
Cross-Site Request Forgery (CSRF)	18-Dec-2022	8.8	A vulnerability classified as problematic was found in wp-english-wp-admin Plugin up to 1.5.1. Affected by this vulnerability is the function register_endpoints of the file english-wp-admin.php. The manipulation leads to cross-site request forgery. The attack can be launched remotely. Upgrading to version 1.5.2 is able to address this issue. The name of the patch is ad4ba171c974c65c3456e7c6228f59f40783b33d. It is recommended	https://github.com/khromov/wp-english-wp-admin/commit/ad4ba171c974c65c3456e7c6228f59f40783b33d	A-WP--WP-E-090123/593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to upgrade the affected component. The associated identifier of this vulnerability is VDB-216199. **CVE ID : CVE-2022-4604**		
Vendor: wphowto					
Product: flowplayer_video_player					
Affected Version(s): * Up to (excluding) 1.0.5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	The Flowplayer Video Player WordPress plugin before 1.0.5 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2022-3984**	N/A	A-WPH-FLOW-090123/594
Product: videojs_html5_player					
Affected Version(s): * Up to (excluding) 1.1.9					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-Dec-2022	5.4	The Videojs HTML5 Player WordPress plugin before 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks **CVE ID : CVE-2022-3985**	N/A	A-WPH-VIDE-090123/595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: wpvar					
Product: wp_shamsi					
Affected Version(s): * Up to (excluding) 4.1.1					
Missing Authorization	16-Dec-2022	5.3	The WP Shamsi plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the deactivate() function hooked via init() in versions up to, and including, 4.1.0. This makes it possible for unauthenticated attackers to deactivate arbitrary plugins on the site. This can be used to deactivate security plugins that aids in exploiting other vulnerabilities. **CVE ID : CVE-2022-4555**	N/A	A-WPV-WP_S-090123/596
Vendor: wpwax					
Product: directorist					
Affected Version(s): * Up to (excluding) 7.4.4					
Missing Authorization	19-Dec-2022	6.5	The Directorist WordPress plugin before 7.4.4 does not prevent users with low privileges (like subscribers) from accessing sensitive system information. **CVE ID : CVE-2022-3961**	N/A	A-WPW-DIRE-090123/597
Vendor: xml-rpc.net_project					
Product: xml-rpc.net					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 2.5.0					
Improper Restriction of XML External Entity Reference	18-Dec-2022	8.8	An XML external entity (XXE) injection vulnerability in XML-RPC.NET before 2.5.0 allows remote authenticated users to conduct server-side request forgery (SSRF) attacks, as demonstrated by a pingback.aspx POST request. **CVE ID : CVE-2022-47514**	https://papercutsoftware.github.io/XML-RPC.NET/download.html	A-XML-XML--090123/598
Vendor: Zenphoto					
Product: Zenphoto					
Affected Version(s): * Up to (excluding) 1.6					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Dec-2022	4.8	Stored cross-site scripting vulnerability in Zenphoto versions prior to 1.6 allows remote a remote authenticated attacker with an administrative privilege to inject an arbitrary script. **CVE ID : CVE-2022-44449**	https://www.zenphoto.org/	A-ZEN-ZENP-090123/599
Vendor: znote					
Product: znote					
Affected Version(s): * Up to (excluding) 1.7.11					
Improper Neutralization of Input During Web Page Generation	19-Dec-2022	5.4	Cross-site Scripting (XSS) - Stored in GitHub repository alagrede/znote-app prior to 1.7.11. **CVE ID : CVE-2022-4614**	https://huntr.dev/bounties/8b429330-3096-4fe4-85e0-1a9143e4dca5, https://gith	A-ZNO-ZNOT-090123/600

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')				ub.com/alagrede/znote-app/commit/d889337b9c3ed16ca1aa43837af0960321dd77f2	
Vendor: Zohocorp					
Product: manageengine_device_control_plus					
Affected Version(s): 10.1.2228.15					
N/A	20-Dec-2022	7.8	** DISPUTED ** An issue was discovered in the endpoint protection agent in Zoho ManageEngine Device Control Plus 10.1.2228.15. Despite configuring complete restrictions on USB pendrives, USB HDD devices, memory cards, USB connections to mobile devices, etc., it is still possible to bypass the USB restrictions by making use of a virtual machine (VM). This allows a file to be exchanged outside the laptop/system. VMs can be created by any user (even without admin rights). The data exfiltration can occur without any record in the audit trail of Windows events on the host machine. NOTE: the vendor's position is "it's not a vulnerability in our product."	https://www.manageengine.com/device-control/how-to/device-control.html	A-ZOH-MANA-090123/601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-47577		
N/A	20-Dec-2022	7.8	** DISPUTED ** An issue was discovered in the endpoint protection agent in Zoho ManageEngine Device Control Plus 10.1.2228.15. Despite configuring complete restrictions on USB pendrives, USB HDD devices, memory cards, USB connections to mobile devices, etc., it is still possible to bypass the USB restrictions by booting into Safe Mode. This allows a file to be exchanged outside the laptop/system. Safe Mode can be launched by any user (even without admin rights). Data exfiltration can occur, and also malware might be introduced onto the system. NOTE: the vendor's position is "it's not a vulnerability in our product." **CVE ID : CVE-2022-47578**	https://www.manageengine.com/device-control/how-to/device-control.html	A-ZOH-MANA-090123/602
Hardware					
Vendor: AMD					
Product: amd64					
Affected Version(s): -					
N/A	20-Dec-2022	8.8	A vulnerability in the label-based access control of Grafana Labs Grafana Enterprise Metrics allows an	https://grafana.com/docs/enterprise-metrics/v2.4	H-AMD-AMD6-100123/603

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attacker more access than intended. If an access policy which has label selector restrictions also has been granted access to all tenants in the system, the label selector restrictions will not be applied when using this policy with the affected versions of the software. This issue affects: Grafana Labs Grafana Enterprise Metrics GEM 1.X versions prior to 1.7.1 on AMD64; GEM 2.X versions prior to 2.3.1 on AMD64. **CVE ID : CVE-2022-44643**	.x/downloads/#v171----november-14th-2022, https://grafana.com/docs/enterprise-metrics/v2.4.x/downloads/#v231----november-14th-2022	
Vendor: Buffalo					
Product: wcr-1166ds					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WCR--100123/604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier,	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WCR--100123/605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wex-1800ax4					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WEX--100123/606

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WEX--100123/607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wex-1800ax4ea					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WEX--100123/608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WEX--100123/609

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-2533dhp					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page.	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43443		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device.	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43486		
Product: wsr-2533dhp2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/612
Improper Neutralization of	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and	https://www.buffalo.jp/news/detail	H-BUF-WSR--100123/613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**	/20221205-01.html	
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-2533dhp3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/615

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-2533dhpl					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/618

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-2533dhpl2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/621

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wsr-2533dhpls					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/623
Improper Neutralization of Special Elements used in an	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/624

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier,	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-3200ax4b					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier,	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier,	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/627

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-3200ax4s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver.	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program.	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/630

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43466		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device.	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43486		
Product: wsr-a2533dhp2					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/632
Improper Neutralization of	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and	https://www.buffalo.jp/news/detail	H-BUF-WSR--100123/633

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**	/20221205-01.html	
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-a2533dhp3					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/636

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS	https://www.buffalo.jp/news/detail/20221205-01.html	H-BUF-WSR--100123/637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Vendor: Dataprobe					
Product: iboot-pdu4-n20					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/638
Improper Limitation of a Pathname to a Restricted Directory	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/639

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**		
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/640
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/641
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/642

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**		
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/643
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			specified in the changed host parameter. **CVE ID : CVE-2022-3189**		
Product: iboot-pdu4a-n15					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/645
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/646
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**		
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/648
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/649
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**		
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/651
Product: iboot-pdu4a-n20					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			command injection vulnerability. **CVE ID : CVE-2022-3183**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/653
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/654
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**		
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/656
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/657
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**		
Product: iboot-pdu4sa-n15					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/659
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/660

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to write a file to the webroot directory. **CVE ID : CVE-2022-3184**		
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/661
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/662
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/663

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**		
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/664
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: iboot-pdu4sa-n20					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/666
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/667
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**		
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/669
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/670
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**		
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/672
Product: iboot-pdu8a-2n15					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/674
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/675
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/677
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/678
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**		
Product: iboot-pdu8a-2n20					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/680
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/681

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/682
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/683
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/684

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3187		
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/685
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/686
Product: iboot-pdu8a-n15					
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')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/687
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/688
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other device's information. **CVE ID : CVE-2022-3186**		
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/690
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/691
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			completed by specific users. **CVE ID : CVE-2022-3188**		
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/693
Product: iboot-pdu8a-n20					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/694
Improper Limitation	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to	https://www.cisa.gov/u	H-DAT-IBOO-100123/695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	scert/ics/advisories/icsa-22-263-03	
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/696
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/698
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/699
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**		
Product: iboot-pdu8sa-2n15					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/701
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/702

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/703
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/704
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/705

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3187		
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/706
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/707
Product: iboot-pdu8sa-n15					
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')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/708
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/709
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other device's information. **CVE ID : CVE-2022-3186**		
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/711
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/712
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/713

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			completed by specific users. **CVE ID : CVE-2022-3188**		
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/714
Product: iboot-pdu8sa-n20					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/715
Improper Limitation	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to	https://www.cisa.gov/u	H-DAT-IBOO-100123/716

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	scert/ics/advisories/icsa-22-263-03	
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/717
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/718

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/719
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/720
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	H-DAT-IBOO-100123/721

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**		
Vendor: Dlink					
Product: dap-2310					
Affected Version(s): -					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**	https://www.dlink.com/en/security-bulletin/	H-DLI-DAP--100123/722
Product: dap-2330					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**	https://www.dlink.com/en/security-bulletin/	H-DLI-DAP--100123/723
Product: dap-2360					
Affected Version(s): -					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier	https://www.dlink.com/en/security-bulletin/	H-DLI-DAP--100123/724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**		
Product: dap-2553					
Affected Version(s): -					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**	https://www.dlink.com/en/security-bulletin/	H-DLI-DAP--100123/725
Product: dap-2660					
Affected Version(s): -					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330	https://www.dlink.com	H-DLI-DAP--100123/726

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**	/en/security-bulletin/	
Product: dap-2690					
Affected Version(s): -					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via	https://www.dlink.com/en/security-bulletin/	H-DLI-DAP--100123/727

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**		
Product: dap-2695					
Affected Version(s): -					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**	https://www.dlink.com/en/security-bulletin/	H-DLI-DAP--100123/728
Product: dap-3320					
Affected Version(s): -					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553	https://www.dlink.com/en/security-bulletin/	H-DLI-DAP--100123/729

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**		
Product: dap-3662					
Affected Version(s): -					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after	https://www.dlink.com/en/security-bulletin/	H-DLI-DAP--100123/730

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the firmware header. **CVE ID : CVE-2022-38873**		
Product: dir-846					
Affected Version(s): a1					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Dec-2022	9.9	D-Link DIR-846 A1_FW100A43 was discovered to contain a command injection vulnerability via the lan(0)_dhcps_staticlist parameter in the SetIpMacBindSettings function. **CVE ID : CVE-2022-46641**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--100123/731
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Dec-2022	9.9	D-Link DIR-846 A1_FW100A43 was discovered to contain a command injection vulnerability via the auto_upgrade_hour parameter in the SetAutoUpgradeInfo function. **CVE ID : CVE-2022-46642**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--100123/732
Product: dir-869					
Affected Version(s): -					
Incorrect Authorization	20-Dec-2022	7.5	D-Link DIR-869 DIR869Ax_FW102B15 is vulnerable to Authentication Bypass via phpcgi. **CVE ID : CVE-2022-46076**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--100123/733
Product: dir-869ax					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	20-Dec-2022	7.5	D-Link DIR-869 DIR869Ax_FW102B15 is vulnerable to Authentication Bypass via phpcgi. **CVE ID : CVE-2022-46076**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--100123/734
Vendor: Hikvision					
Product: ds-3wf01c-2n\/o					
Affected Version(s): -					
N/A	19-Dec-2022	9.8	The web server of some Hikvision wireless bridge products have an access control vulnerability which can be used to obtain the admin permission. The attacker can exploit the vulnerability by sending crafted messages to the affected devices. **CVE ID : CVE-2022-28173**	https://www.hikvision.com/en/support/cybersecurity/security-advisory/access-control-vulnerability-in-some-hikvision-wireless-bridge-products/	H-HIK-DS-3-100123/735
Product: ds-3wf0ac-2nt					
Affected Version(s): -					
N/A	19-Dec-2022	9.8	The web server of some Hikvision wireless bridge products have an access control vulnerability which can be used to obtain the admin permission. The attacker can exploit the vulnerability by sending crafted messages to the affected devices. **CVE ID : CVE-2022-28173**	https://www.hikvision.com/en/support/cybersecurity/security-advisory/access-control-vulnerability-in-some-hikvision-wireless-bridge-products/	H-HIK-DS-3-100123/736

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Microchip					
Product: bm64					
Affected Version(s): -					
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM64-100123/737
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM64-100123/738
Product: bm70					
Affected Version(s): -					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages.	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-	H-MIC-BM70-100123/739

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46403	response/deviating-behaviors-in-bluetooth-le	
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM70-100123/740
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM70-100123/741
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing.	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/de	H-MIC-BM70-100123/742

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46400	viating-behaviors-in-bluetooth-le	
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM70-100123/743
Product: bm71					
Affected Version(s): -					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM71-100123/744
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero.	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability	H-MIC-BM71-100123/745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46399	-response/deviating-behaviors-in-bluetooth-le	
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM71-100123/746
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM71-100123/747
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete.	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-	H-MIC-BM71-100123/748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46401	response/deviating-behaviors-in-bluetooth-le	
Product: bm77					
Affected Version(s): -					
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM77-100123/749
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM77-100123/750
Product: bm78					
Affected Version(s): -					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112)	https://www.microchip.com/en-us/products/wireless-	H-MIC-BM78-100123/751

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mishandles reject messages. **CVE ID : CVE-2022-46403**	connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM78-100123/752
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM78-100123/753
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to	https://www.microchip.com/en-us/products/wireless-connectivity	H-MIC-BM78-100123/754

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM78-100123/755
Product: bm83					
Affected Version(s): -					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM83-100123/756
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer	https://www.microchip.com/en-us/products	H-MIC-BM83-100123/757

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM83-100123/758
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-BM83-100123/759
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112)	https://www.microchip.com/en-us/products/wireless-	H-MIC-BM83-100123/760

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	connectivity /software-vulnerability - response/deviating-behaviors-in-bluetooth-le	
Product: is1870					
Affected Version(s): -					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-IS18-100123/761
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-IS18-100123/762
Improper Validation of Integrity	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC	https://www.microchip.com/en-	H-MIC-IS18-100123/763

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Check Value			LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-IS18-100123/764
Product: is1871					
Affected Version(s): -					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-IS18-100123/765

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-IS18-100123/766
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-IS18-100123/767
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-IS18-100123/768
Product: pic32cx1012bz25048					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-PIC3-100123/769
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-PIC3-100123/770
Product: pic_lightblue_explorer_demo					
Affected Version(s): -					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-	H-MIC-PIC_-100123/771

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				behaviors-in-bluetooth-le	
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-PIC_-100123/772
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-PIC_-100123/773
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-	H-MIC-PIC_-100123/774

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				in-bluetooth-le	
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-PIC_-100123/775
Product: rn4678					
Affected Version(s): -					
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-RN46-100123/776
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete.	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/de	H-MIC-RN46-100123/777

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46401	viating-behaviors-in-bluetooth-le	
Product: rn4870					
Affected Version(s): -					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-RN48-100123/778
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-RN48-100123/779
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values.	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability	H-MIC-RN48-100123/780

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46402	-response/deviating-behaviors-in-bluetooth-le	
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-RN48-100123/781
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-RN48-100123/782
Product: rn4871					
Affected Version(s): -					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112)	https://www.microchip.com/en-us/products/wireless-connectivity	H-MIC-RN48-100123/783

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			mishandles reject messages. **CVE ID : CVE-2022-46403**	/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-RN48-100123/784
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-RN48-100123/785
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to	https://www.microchip.com/en-us/products/wireless-connectivity/software-	H-MIC-RN48-100123/786

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	vulnerability-response/deviating-behaviors-in-bluetooth-le	
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-RN48-100123/787
Product: wbz451					
Affected Version(s): -					
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	H-MIC-WBZ4-100123/788
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112)	https://www.microchip.com/en-us/products/wireless-	H-MIC-WBZ4-100123/789

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	connectivity /software-vulnerability - response/deviating-behaviors-in-bluetooth-le	
Vendor: Netgear					
Product: nighthawk_ax11000					
Affected Version(s): -					
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication. **CVE ID : CVE-2022-47208**	https://www.tenable.com/security/research/tra-2022-37	H-NET-NIGH-100123/790
Product: nighthawk_ax1800					
Affected Version(s): -					
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on	https://www.tenable.com/security/research/tra-2022-37	H-NET-NIGH-100123/791

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the device without authentication. **CVE ID : CVE-2022-47208**		
Product: nighthawk_ax2400					
Affected Version(s): -					
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication. **CVE ID : CVE-2022-47208**	https://www.tenable.com/security/research/tra-2022-37	H-NET-NIGH-100123/792
Product: nighthawk_ax3000					
Affected Version(s): -					
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication. **CVE ID : CVE-2022-47208**	https://www.tenable.com/security/research/tra-2022-37	H-NET-NIGH-100123/793
Product: nighthawk_ax5400					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication. **CVE ID : CVE-2022-47208**	https://www.tenable.com/security/research/tra-2022-37	H-NET-NIGH-100123/794
Product: nighthawk_ax6000					
Affected Version(s): -					
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication. **CVE ID : CVE-2022-47208**	https://www.tenable.com/security/research/tra-2022-37	H-NET-NIGH-100123/795
Product: rax30					
Affected Version(s): -					
Use of Hard-coded Credentials	16-Dec-2022	8.8	A support user exists on the device and appears to be a backdoor for Technical Support staff. The default password for this account is "support" and cannot	https://www.tenable.com/security/research/tra-2022-37	H-NET-RAX3-100123/796

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			be changed by a user via any normally accessible means. **CVE ID : CVE-2022-47209**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.8	The default console presented to users over telnet (when enabled) is restricted to a subset of commands. Commands issued at this console, however, appear to be fed directly into a system call or other similar function. This allows any authenticated user to execute arbitrary commands on the device. **CVE ID : CVE-2022-47210**	https://www.tenable.com/security/research/tra-2022-37	H-NET-RAX3-100123/797
Product: wnr2000					
Affected Version(s): 1.0					
N/A	20-Dec-2022	8.1	An exploitable firmware modification vulnerability was discovered on the Netgear WNR2000v1 router. An attacker can conduct a MITM (Man-in-the-Middle) attack to modify the user-uploaded firmware image and bypass the CRC check, allowing attackers to execute arbitrary code or cause a Denial of Service (DoS). This affects v1.2.3.7 and earlier.	https://www.netgear.com/about/security/	H-NET-WNR2-100123/798

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46423		
N/A	20-Dec-2022	4.8	An issue in Netgear WNR2000 v1 1.2.3.7 and earlier allows authenticated attackers to cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46422**	https://www.netgear.com/about/security/	H-NET-WNR2-100123/799
Product: xwn5001					
Affected Version(s): -					
N/A	20-Dec-2022	8.1	An exploitable firmware modification vulnerability was discovered on the Netgear XWN5001 Powerline 500 WiFi Access Point. An attacker can conduct a MITM (Man-in-the-Middle) attack to modify the user-uploaded firmware image and bypass the CRC check, allowing attackers to execute arbitrary code or cause a Denial of Service (DoS). This affects v0.4.1.1 and earlier. **CVE ID : CVE-2022-46424**	https://www.netgear.com/about/security/	H-NET-XWN5-100123/800
Vendor: Nokia					
Product: fastmile					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	21-Dec-2022	8.4	Nokia Fastmile 3tg00118abad52 devices shipped by Optus are shipped with a default hardcoded admin account of admin:Nq+L5st7o This account can be used locally to access the web admin interface. **CVE ID : CVE-2022-36222**	N/A	H-NOK-FAST-100123/801
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	6.5	Nokia Fastmile 3tg00118abad52 is affected by an authenticated path traversal vulnerability which allows attackers to read any named pipe file on the system. **CVE ID : CVE-2022-36221**	N/A	H-NOK-FAST-100123/802
Vendor: paxtechnology					
Product: a930					
Affected Version(s): -					
Improper Input Validation	16-Dec-2022	7.8	The systool_server in PAX Technology A930 PayDroid 7.1.1 Virgo V04.4.02 20211201 fails to check for dollar signs or backticks in user supplied commands, leading to to arbitrary command execution as root. **CVE ID : CVE-2022-26582**	N/A	H-PAX-A930-100123/803
Improper Neutralization of Special	16-Dec-2022	6.8	PAX Technology A930 PayDroid 7.1.1 Virgo V04.4.02 20211201 was discovered to be	N/A	H-PAX-A930-100123/804

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			vulnerable to command injection. **CVE ID : CVE-2022-26580**		
Missing Authorization	16-Dec-2022	6.8	The ADB daemon in PAX Technology A930 PayDroid 7.1.1 Virgo V04.4.02 20211201 allows the execution of the systool utility in production mode, allowing unauthenticated attackers to perform privileged actions. **CVE ID : CVE-2022-26581**	N/A	H-PAX-A930-100123/805
Insufficient Verification of Data Authenticity	16-Dec-2022	6	PAX Technology A930 PayDroid 7.1.1 Virgo V04.4.02 20211201 allows root privileged attackers to install an unsigned application by copying the APK to /data/app, setting the appropriate permissions and rebooting the device. **CVE ID : CVE-2022-26579**	N/A	H-PAX-A930-100123/806
Vendor: Rockwellautomation					
Product: compactlogix_5370					
Affected Version(s): -					
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request	https://rockwellautomation.custhelp.com/app/answers/answ	H-ROC-COMP-100123/807

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS). **CVE ID : CVE-2022-3157**	er_view/a_id/1137757	
Product: compactlogix_5380					
Affected Version(s): -					
N/A	19-Dec-2022	7.5	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition in Rockwell Automation Logix controllers resulting in a major non-recoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online and continue normal operation. **CVE ID : CVE-2022-3752**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137664	H-ROC-COMP-100123/808
Product: compactlogix_5480					
Affected Version(s): -					
N/A	19-Dec-2022	7.5	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition in Rockwell	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137664	H-ROC-COMP-100123/809

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Automation Logix controllers resulting in a major non-recoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online and continue normal operation. **CVE ID : CVE-2022-3752**		
Product: compactlogix_5580					
Affected Version(s): -					
N/A	19-Dec-2022	7.5	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition in Rockwell Automation Logix controllers resulting in a major non-recoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online and continue normal operation. **CVE ID : CVE-2022-3752**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137664	H-ROC-COMP-100123/810
Product: compact_guardlogix_5370					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS). **CVE ID : CVE-2022-3157**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757	H-ROC-COMP-100123/811
Product: compact_guardlogix_5380					
Affected Version(s): -					
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS). **CVE ID : CVE-2022-3157**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757	H-ROC-COMP-100123/812
N/A	19-Dec-2022	7.5	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition in Rockwell Automation Logix controllers resulting in a major non-recoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137664	H-ROC-COMP-100123/813

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the user project file to bring the device back online and continue normal operation. **CVE ID : CVE-2022-3752**		
Product: controllogix_5570					
Affected Version(s): -					
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS). **CVE ID : CVE-2022-3157**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757	H-ROC-CONT-100123/814
Product: controllogix_5570_redundancy					
Affected Version(s): -					
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS). **CVE ID : CVE-2022-3157**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757	H-ROC-CONT-100123/815
Product: guardlogix_5570					
Affected Version(s): -					
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a	https://rockwellautomation.custhelp.com/app/an	H-ROC-GUAR-100123/816

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS). **CVE ID : CVE-2022-3157**	swers/answer_view/a_id/1137757	
Product: guardlogix_5580					
Affected Version(s): -					
N/A	19-Dec-2022	7.5	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition in Rockwell Automation Logix controllers resulting in a major non-recoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online and continue normal operation. **CVE ID : CVE-2022-3752**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137664	H-ROC-GUAR-100123/817
Product: micrologix_1100					
Affected Version(s): -					
Improper Enforcement of Message Integrity During Transmissi	16-Dec-2022	7.5	Rockwell Automation was made aware that the webservers of the Micrologix 1100 and 1400 controllers contain a vulnerability that may lead to a	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137678	H-ROC-MICR-100123/818

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
on in a Communication Channel			denial-of-service condition. The security vulnerability could be exploited by an attacker with network access to the affected systems by sending TCP packets to webserver and closing it abruptly which would cause a denial-of-service condition for the web server application on the device **CVE ID : CVE-2022-3166**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Rockwell Automation was made aware of a vulnerability by a security researcher from Georgia Institute of Technology that the MicroLogix 1100 and 1400 controllers contain a vulnerability that may give an attacker the ability to accomplish remote code execution. The vulnerability is an unauthenticated stored cross-site scripting vulnerability in the embedded webserver. The payload is transferred to the controller over SNMP and is rendered on the homepage of the embedded website. **CVE ID : CVE-2022-46670**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137679	H-ROC-MICR-100123/819

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: micrologix_1400					
Affected Version(s): -					
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	16-Dec-2022	7.5	Rockwell Automation was made aware that the webservers of the Micrologix 1100 and 1400 controllers contain a vulnerability that may lead to a denial-of-service condition. The security vulnerability could be exploited by an attacker with network access to the affected systems by sending TCP packets to webserver and closing it abruptly which would cause a denial-of-service condition for the web server application on the device **CVE ID : CVE-2022-3166**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137678	H-ROC-MICR-100123/820
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Rockwell Automation was made aware of a vulnerability by a security researcher from Georgia Institute of Technology that the MicroLogix 1100 and 1400 controllers contain a vulnerability that may give an attacker the ability to accomplish remote code execution. The vulnerability is an unauthenticated stored cross-site scripting vulnerability in the embedded webserver.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137679	H-ROC-MICR-100123/821

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The payload is transferred to the controller over SNMP and is rendered on the homepage of the embedded website. **CVE ID : CVE-2022-46670**		
Product: micrologix_1400-a					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Rockwell Automation was made aware of a vulnerability by a security researcher from Georgia Institute of Technology that the MicroLogix 1100 and 1400 controllers contain a vulnerability that may give an attacker the ability to accomplish remote code execution. The vulnerability is an unauthenticated stored cross-site scripting vulnerability in the embedded webserver. The payload is transferred to the controller over SNMP and is rendered on the homepage of the embedded website. **CVE ID : CVE-2022-46670**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137679	H-ROC-MICR-100123/822
Product: micrologix_1400-b					
Affected Version(s): -					
Improper Neutralization of	16-Dec-2022	6.1	Rockwell Automation was made aware of a vulnerability by a	https://rockwellautomation.custhelp.	H-ROC-MICR-100123/823

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input During Web Page Generation ('Cross-site Scripting')			security researcher from Georgia Institute of Technology that the MicroLogix 1100 and 1400 controllers contain a vulnerability that may give an attacker the ability to accomplish remote code execution. The vulnerability is an unauthenticated stored cross-site scripting vulnerability in the embedded webserver. The payload is transferred to the controller over SNMP and is rendered on the homepage of the embedded website. **CVE ID : CVE-2022-46670**	com/app/answers/answer_view/a_id/1137679	
Product: micrologix_1400-c					
Affected Version(s): -					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Rockwell Automation was made aware of a vulnerability by a security researcher from Georgia Institute of Technology that the MicroLogix 1100 and 1400 controllers contain a vulnerability that may give an attacker the ability to accomplish remote code execution. The vulnerability is an unauthenticated stored cross-site scripting vulnerability in the embedded webserver.	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137679	H-ROC-MICR-100123/824

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			The payload is transferred to the controller over SNMP and is rendered on the homepage of the embedded website. **CVE ID : CVE-2022-46670**		
Vendor: Sharp					
Product: bp-30c25					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-3-100123/825
Product: bp-30c25t					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-3-100123/826

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-30c25y					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-3-100123/827

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-30c25z					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-3-100123/828
Product: bp-30m28					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-3-100123/829

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-30m28t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-3-100123/830

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-30m31					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-3-100123/831
Product: bp-30m31t					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-3-100123/832

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-30m35					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-3-100123/833

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-30m35t					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-3-100123/834
Product: bp-50c26					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-5-100123/835

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-50c31					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-5-100123/836

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50c36					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-5-100123/837
Product: bp-50c45					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-5-100123/838

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-50c55					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-5-100123/839

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50c65					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-5-100123/840
Product: bp-50m26					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-5-100123/841

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-50m31					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-5-100123/842

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50m36					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-5-100123/843
Product: bp-50m45					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-5-100123/844

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-50m50					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-5-100123/845

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50m55					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-5-100123/846
Product: bp-55c26					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-5-100123/847

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-60c31					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-6-100123/848

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-60c36					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-6-100123/849
Product: bp-60c45					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-6-100123/850

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-70c31					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-7-100123/851

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70c36					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-7-100123/852
Product: bp-70c45					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-7-100123/853

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-70c55					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-7-100123/854

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70c65					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-7-100123/855
Product: bp-70m31					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-7-100123/856

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-70m36					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-7-100123/857

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70m45					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-7-100123/858
Product: bp-70m55					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-7-100123/859

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: bp-70m65					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-7-100123/860

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70m75					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-BP-7-100123/861
Product: bp-70m90					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-BP-7-100123/862

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-2630n					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-2-100123/863

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-2651					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-2-100123/864
Product: mx-3050n					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-3-100123/865

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-3050n_a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/866

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3050v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/867
Product: mx-3050v_a					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-3-100123/868

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-3051					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/869

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3060n					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/870
Product: mx-3060v					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-3-100123/871

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-3061					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/872

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3061s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/873
Product: mx-3070n					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-3-100123/874

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-3070n_a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/875

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3070v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/876
Product: mx-3070v_a					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-3-100123/877

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-3071					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/878

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3071s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/879
Product: mx-3550n					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-3-100123/880

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-3550v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/881

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3551					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/882
Product: mx-3560n					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-3-100123/883

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-3560v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/884

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3561					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/885
Product: mx-3561s					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-3-100123/886

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-3570n					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/887

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3570v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/888
Product: mx-3571					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-3-100123/889

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-3571s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-3-100123/890

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4050n					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-4-100123/891
Product: mx-4050v					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-4-100123/892

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-4051					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-4-100123/893

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4060n					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-4-100123/894
Product: mx-4060v					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-4-100123/895

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-4061					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-4-100123/896

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4061s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-4-100123/897
Product: mx-4070n					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-4-100123/898

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-4070n_a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-4-100123/899

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4070v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-4-100123/900
Product: mx-4070v_a					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-4-100123/901

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-4071					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-4-100123/902

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4071s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-4-100123/903
Product: mx-5050n					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-5-100123/904

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-5050v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-5-100123/905

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-5051					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-5-100123/906
Product: mx-5070n					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-5-100123/907

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-5070v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-5-100123/908

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-5071					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-5-100123/909
Product: mx-5071s					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-5-100123/910

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-6050n					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-6-100123/911

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-6050v					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-6-100123/912
Product: mx-6051					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-6-100123/913

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-6070n					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-6-100123/914

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-6070n_a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-6-100123/915
Product: mx-6070v					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-6-100123/916

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-6070v_a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-6-100123/917

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-6071					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-6-100123/918
Product: mx-6071s					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-6-100123/919

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-6580n					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-6-100123/920

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-7081					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-7-100123/921
Product: mx-7090n					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-7-100123/922

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-7580n					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-7-100123/923

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-8081					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-8-100123/924
Product: mx-8090n					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-8-100123/925

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-b355w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-B-100123/926

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b355wt					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-B-100123/927
Product: mx-b355wz					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-B-100123/928

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-b356w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-B-100123/929

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b356wh					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-B-100123/930
Product: mx-b376w					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-B-100123/931

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-b376wh					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-B-100123/932

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b455w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-B-100123/933
Product: mx-b455wt					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-B-100123/934

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-b455wz					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-B-100123/935

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b456w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-B-100123/936
Product: mx-b456wh					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-B-100123/937

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-b476w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-B-100123/938

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b476wh					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-B-100123/939
Product: mx-c303					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-C-100123/940

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-c303w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-C-100123/941

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-c303wh					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-C-100123/942
Product: mx-c304					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-C-100123/943

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-c304w					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-C-100123/944

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-c304wh					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-C-100123/945
Product: mx-m1056					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/946

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m1206					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/947

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m2630					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/948
Product: mx-m2630_a					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/949

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m2651					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/950

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3050					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/951
Product: mx-m3050_a					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/952

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m3051					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/953

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3070					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/954
Product: mx-m3070_a					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/955

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m3071					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/956

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3071s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/957
Product: mx-m3550					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/958

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m3551					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/959

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3570					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/960
Product: mx-m3571					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/961

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m3571s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/962

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m4050					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/963
Product: mx-m4051					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/964

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m4070					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/965

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m4070_a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/966
Product: mx-m4071					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/967

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m4071s					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/968

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m5050					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/969
Product: mx-m5051					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/970

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m5070					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/971

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m5071					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/972
Product: mx-m5071s					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/973

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m6050					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/974

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m6051					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/975
Product: mx-m6070					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/976

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m6070_a					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/977

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m6071					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/978
Product: mx-m6071s					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/979

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Product: mx-m6570					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/980

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m7570					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	H-SHA-MX-M-100123/981
Product: mx-m905					
Affected Version(s): -					
Improper Neutralizat	16-Dec-2022	7.2	Command injection vulnerability in	https://global.sharp/pro	H-SHA-MX-M-100123/982

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in a Command ('Command Injection')			nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	ducts/copier/info/info_security_2022-11.html	
Vendor: sick					
Product: sim2000st					
Affected Version(s): -					
Weak Password Recovery Mechanism for Forgotten Password	16-Dec-2022	9.8	Password recovery vulnerability in SICK SIM2000ST Partnumber 2086502 with firmware version <1.13.4 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an	https://sick.com/psirt	H-SIC-SIM2-100123/983

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 1.13.4 as soon as possible (available in SICK Support Portal). **CVE ID : CVE-2022-47377**		
Vendor: Tenda					
Product: ac10					
Affected Version(s): -					
Out-of-bounds Write	16-Dec-2022	7.5	Tenda AC15 V15.03.06.23 is vulnerable to Buffer Overflow via function formSetClientState. **CVE ID : CVE-2022-46109**	N/A	H-TEN-AC10-100123/984
Product: f1203					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Dec-2022	9.8	Tenda F1203 V2.0.1.6 was discovered to contain a command injection vulnerability via the mac parameter at /goform/WriteFacMac. **CVE ID : CVE-2022-46538**	N/A	H-TEN-F120-100123/985

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the mac parameter at /goform/GetParentControlInfo. **CVE ID : CVE-2022-46530**	N/A	H-TEN-F120-100123/986
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the deviceId parameter at /goform/addWifiMacFilter. **CVE ID : CVE-2022-46531**	N/A	H-TEN-F120-100123/987
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the deviceMac parameter at /goform/addWifiMacFilter. **CVE ID : CVE-2022-46532**	N/A	H-TEN-F120-100123/988
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the limitSpeed parameter at /goform/SetClientState. **CVE ID : CVE-2022-46533**	N/A	H-TEN-F120-100123/989
Buffer Copy without Checking Size of	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the	N/A	H-TEN-F120-100123/990

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			speed_dir parameter at /goform/SetSpeedWan. **CVE ID : CVE-2022-46534**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the deviceId parameter at /goform/SetClientState. **CVE ID : CVE-2022-46535**	N/A	H-TEN-F120-100123/991
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the limitSpeedUp parameter at /goform/SetClientState. **CVE ID : CVE-2022-46536**	N/A	H-TEN-F120-100123/992
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the security parameter at /goform/WifiBasicSet. **CVE ID : CVE-2022-46537**	N/A	H-TEN-F120-100123/993
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the security_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2022-46539**	N/A	H-TEN-F120-100123/994

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the entrys parameter at /goform/addressNat. **CVE ID : CVE-2022-46540**	N/A	H-TEN-F120-100123/995
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the ssid parameter at /goform/fast_setting_wifi_set. **CVE ID : CVE-2022-46541**	N/A	H-TEN-F120-100123/996
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the page parameter at /goform/addressNat. **CVE ID : CVE-2022-46542**	N/A	H-TEN-F120-100123/997
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the mitInterface parameter at /goform/addressNat. **CVE ID : CVE-2022-46543**	N/A	H-TEN-F120-100123/998
Buffer Copy without Checking Size of Input	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the cmdinput parameter at /goform/exeCommand.	N/A	H-TEN-F120-100123/999

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2022-46544**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the page parameter at /goform/NatStaticSetting. **CVE ID : CVE-2022-46545**	N/A	H-TEN-F120-100123/1000
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the entrys parameter at /goform/RouteStatic. **CVE ID : CVE-2022-46546**	N/A	H-TEN-F120-100123/1001
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the page parameter at /goform/VirtualSer. **CVE ID : CVE-2022-46547**	N/A	H-TEN-F120-100123/1002
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the page parameter at /goform/DhcpListClient. **CVE ID : CVE-2022-46548**	N/A	H-TEN-F120-100123/1003
Buffer Copy without	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer	N/A	H-TEN-F120-100123/1004

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			overflow via the deviceId parameter at /goform/saveParentControlInfo. **CVE ID : CVE-2022-46549**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the urls parameter at /goform/saveParentControlInfo. **CVE ID : CVE-2022-46550**	N/A	H-TEN-F120-100123/1005
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the time parameter at /goform/saveParentControlInfo. **CVE ID : CVE-2022-46551**	N/A	H-TEN-F120-100123/1006
Product: i22					
Affected Version(s): -					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the funcpara1 parameter in the formSetCfm function. **CVE ID : CVE-2022-45665**	N/A	H-TEN-I22-100123/1007
Buffer Copy without Checking Size of Input	20-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the list parameter in the	N/A	H-TEN-I22-100123/1008

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			formwrlSSIDset function. **CVE ID : CVE-2022-45666**		
Vendor: Tp-link					
Product: tl-wa7510n_v1					
Affected Version(s): -					
N/A	20-Dec-2022	7.5	An issue in the firmware update process of TP-Link TL-WA7510N v1 v3.12.6 and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46434**	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1009
Product: tl-wa801n					
Affected Version(s): -					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-LINK TL-WA801N / TL-WA801ND V1 v3.12.16 and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46914**	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1010
Product: tl-wa801nd_v1					
Affected Version(s): -					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-LINK TL-	https://www.tp-link.com/us	H-TP--TL-W-100123/1011

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			WA801N / TL-WA801ND V1 v3.12.16 and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46914**	/press/security-advisory/	
Product: tl-wa901n					
Affected Version(s): -					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WA901ND V1 up to v3.11.2 and TL-WA901N V2 up to v3.12.16 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46910**	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1012
Product: tl-wa901nd_v1					
Affected Version(s): -					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WA901ND V1 up to v3.11.2 and TL-WA901N V2 up to v3.12.16 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image.	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1013

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46910		
Product: tl-wa901nd_v2					
Affected Version(s): -					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WA901ND V1 up to v3.11.2 and TL-WA901N V2 up to v3.12.16 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46910**	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1014
Product: tl-wr1043nd_v1					
Affected Version(s): -					
Download of Code Without Integrity Check	20-Dec-2022	4.8	TP-Link TL-WR1043ND V1 3.13.15 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46428**	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1015
Product: tl-wr740n_v1					
Affected Version(s): -					
Download of Code Without Integrity Check	20-Dec-2022	4.8	TP-Link TL-WR740N V1 and V2 v3.12.4 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1016

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46430**		
Product: tl-wr740n_v2					
Affected Version(s): -					
Download of Code Without Integrity Check	20-Dec-2022	4.8	TP-Link TL-WR740N V1 and V2 v3.12.4 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46430**	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1017
Product: tl-wr741nd_v1					
Affected Version(s): -					
Download of Code Without Integrity Check	20-Dec-2022	4.8	TP-Link TL-WR740N V1 and V2 v3.12.4 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46430**	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1018
Product: tl-wr741nd_v2					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Download of Code Without Integrity Check	20-Dec-2022	4.8	TP-Link TL-WR740N V1 and V2 v3.12.4 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46430**	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1019
Product: tl-wr743nd_v1					
Affected Version(s): -					
N/A	20-Dec-2022	7.5	An exploitable firmware modification vulnerability was discovered on TP-Link TL-WR743ND V1. An attacker can conduct a MITM (Man-in-the-Middle) attack to modify the user-uploaded firmware image and bypass the CRC check, allowing attackers to execute arbitrary code or cause a Denial of Service (DoS). This affects v3.12.20 and earlier. **CVE ID : CVE-2022-46432**	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1020
Product: tl-wr841n					
Affected Version(s): -					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WR841N / TL-WA841ND V7 3.13.9	https://www.tp-link.com/us/press/secu	H-TP--TL-W-100123/1021

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46912**	rity-advisory/	
Product: tl-wr841nd_v7					
Affected Version(s): -					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WR841N / TL-WA841ND V7 3.13.9 and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46912**	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1022
Product: tl-wr940n_v4					
Affected Version(s): -					
N/A	20-Dec-2022	6.5	TP-Link TL-WR940N V4 3.16.9 and earlier allows authenticated attackers to cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46139**	N/A	H-TP--TL-W-100123/1023
Product: tl-wr941nd_v2					
Affected Version(s): -					
N/A	20-Dec-2022	8.8	An issue in the firmware update	https://www.tp-	H-TP--TL-W-100123/1024

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			process of TP-Link TL-WR941ND V2/V3 up to 3.13.9 and TL-WR941ND V4 up to 3.12.8 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46435**	link.com/us/press/security-advisory/	
Product: tl-wr941nd_v3					
Affected Version(s): -					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WR941ND V2/V3 up to 3.13.9 and TL-WR941ND V4 up to 3.12.8 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46435**	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1025
Product: tl-wr941nd_v4					
Affected Version(s): -					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WR941ND V2/V3 up to 3.13.9 and TL-WR941ND V4 up to 3.12.8 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via	https://www.tp-link.com/us/press/security-advisory/	H-TP--TL-W-100123/1026

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uploading a crafted firmware image. **CVE ID : CVE-2022-46435**		
Vendor: Zyxel					
Product: nbg7510					
Affected Version(s): -					
N/A	21-Dec-2022	9.8	A DNS misconfiguration was found in Zyxel NBG7510 firmware versions prior to V1.00(ABZY.3)C0, which could allow an unauthenticated attacker to access the DNS server when the device is switched to the AP mode. **CVE ID : CVE-2022-38546**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-dns-misconfiguration-in-nbg7510-home-router	H-ZYX-NBG7-100123/1027
Operating System					
Vendor: Apple					
Product: iphone_os					
Affected Version(s): -					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2022	9.8	The search term could have been specified externally to trigger SQL injection. This vulnerability affects Firefox for iOS < 101. **CVE ID : CVE-2022-1887**	https://bugzilla.mozilla.org/show_bug.cgi?id=1767205, https://www.mozilla.org/security/advisories/mfsa2022-23/	O-APP-IPHO-100123/1028
Product: macos					
Affected Version(s): -					
N/A	22-Dec-2022	7.8	When saving or opening an email	https://www.mozilla.or	O-APP-MACO-100123/1029

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			attachment on macOS, Thunderbird did not set attribute com.apple.quarantine on the received file. If the received file was an application and the user attempted to open it, then the application was started immediately without asking the user to confirm. This vulnerability affects Thunderbird < 102.3. **CVE ID : CVE-2022-3155**	g/security/advisories/mfsa2022-42/, https://bugzilla.mozilla.org/show_bug.cgi?id=1789061	
N/A	22-Dec-2022	6.5	By generally accepting and passing resource handles across processes, a compromised content process might have confused higher privileged processes to interact with handles that the unprivileged process should not have access to. *This bug only affects Firefox for Windows and MacOS. Other operating systems are unaffected.*. This vulnerability affects Firefox < 96. **CVE ID : CVE-2022-22750**	https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bug.cgi?id=1566608	O-APP-MACO-100123/1030
N/A	22-Dec-2022	6.5	Previously Firefox for macOS and Linux would download temporary files to a user-specific directory in	https://bugzilla.mozilla.org/show_bug.cgi?id=1752396,	O-APP-MACO-100123/1031

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			<code>/tmp</code>, but this behavior was changed to download them to <code>/tmp</code> where they could be affected by other local users. This behavior was reverted to the original, user-specific directory. *This bug only affects Firefox for macOS and Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.7 and Thunderbird < 91.7. **CVE ID : CVE-2022-26386**	https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/	
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44498**	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	O-APP-MACO-100123/1032
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by	https://helpx.adobe.com/security/products/illust	O-APP-MACO-100123/1033

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44499**	rator/apsb22-60.html	
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44500**	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	O-APP-MACO-100123/1034
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	O-APP-MACO-100123/1035

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44502**		
Vendor: Buffalo					
Product: wcr-1166ds_firmware					
Affected Version(s): * Up to (including) 1.34					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WCR--100123/1036

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request is sent to the management page. **CVE ID : CVE-2022-43443**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WCR--100123/1037

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wex-1800ax4ea_firmware					
Affected Version(s): * Up to (including) 1.13					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WEX--100123/1038

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WEX--100123/1039

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Product: wex-1800ax4_firmware					
Affected Version(s): * Up to (including) 1.13					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WEX--100123/1040
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WEX--100123/1041

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-2533dhp2_firmware					
Affected Version(s): * Up to (including) 1.22					
Improper Neutralization of Special	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B	https://www.buffalo.jp/news/detail	O-BUF-WSR--100123/1042

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**	/20221205-01.html	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1043

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1044

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-2533dhp3_firmware					
Affected Version(s): * Up to (including) 1.26					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1045

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1046

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1047

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-2533dhpl2_firmware					
Affected Version(s): * Up to (including) 1.03					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1048

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request is sent to the management page. **CVE ID : CVE-2022-43443**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1049
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware	https://www.buffalo.jp/news/detail	O-BUF-WSR--100123/1050

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**	/20221205-01.html	
Product: wsr-2533dhpls_firmware					
Affected Version(s): * Up to (including) 1.07					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1051
Improper Neutralization of Special Elements used in an OS Command	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1052

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1053

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-2533dhpl_firmware					
Affected Version(s): * Up to (including) 1.08					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1054

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1055

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-2533dhp_firmware					
Affected Version(s): * Up to (including) 1.08					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1056

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1057

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-3200ax4b_firmware					
Affected Version(s): 1.25					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver.	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1058

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program.	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1059

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43466		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device.	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1060

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43486		
Product: wsr-3200ax4s_firmware					
Affected Version(s): * Up to (including) 1.26					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1061
Improper Neutralization of	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and	https://www.buffalo.jp/news/detail	O-BUF-WSR--100123/1062

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in an OS Command ('OS Command Injection')			earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**	/20221205-01.html	
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1063

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-a2533dhp2_firmware					
Affected Version(s): * Up to (including) 1.22					
Improper Neutralization of Special Elements used in an OS Command ('OS	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1064

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1065

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1066

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Product: wsr-a2533dhp3_firmware					
Affected Version(s): * Up to (including) 1.26					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	8.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1067

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware Ver. 1.07 and earlier, and WCR-1166DS firmware Ver. 1.34 and earlier allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page. **CVE ID : CVE-2022-43443**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	19-Dec-2022	6.8	Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1068

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			request is sent to a specific CGI program. **CVE ID : CVE-2022-43466**		
N/A	19-Dec-2022	6.8	Hidden functionality vulnerability in Buffalo network devices WSR-3200AX4S firmware Ver. 1.26 and earlier, WSR-3200AX4B firmware Ver. 1.25, WSR-2533DHP firmware Ver. 1.08 and earlier, WSR-2533DHP2 firmware Ver. 1.22 and earlier, WSR-A2533DHP2 firmware Ver. 1.22 and earlier, WSR-2533DHP3 firmware Ver. 1.26 and earlier, WSR-A2533DHP3 firmware Ver. 1.26 and earlier, WSR-2533DHPL firmware Ver. 1.08 and earlier, WSR-2533DHPL2 firmware Ver. 1.03 and earlier, WSR-2533DHPLS firmware Ver. 1.07 and earlier, WCR-1166DS firmware Ver. 1.34 and earlier, WEX-1800AX4 firmware Ver. 1.13 and earlier, and WEX-1800AX4EA firmware Ver. 1.13 and earlier allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an	https://www.buffalo.jp/news/detail/20221205-01.html	O-BUF-WSR--100123/1069

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			arbitrary command on the affected device. **CVE ID : CVE-2022-43486**		
Vendor: contiki-ng					
Product: contiki-ng					
Affected Version(s): * Up to (including) 4.8					
NULL Pointer Dereference	16-Dec-2022	6.5	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. Versions prior to 4.9 contain a NULL Pointer Dereference in BLE L2CAP module. The Contiki-NG operating system for IoT devices contains a Bluetooth Low Energy stack. An attacker can inject a packet in this stack, which causes the implementation to dereference a NULL pointer and triggers undefined behavior. More specifically, while processing the L2CAP protocol, the implementation maps an incoming channel ID to its metadata structure. In this structure, state information regarding credits is managed through calls to the function input_l2cap_credit in the module os/net/mac/ble/ble-l2cap.c. Unfortunately,	https://github.com/contiki-ng/contiki-ng/pull/2253	O-CON-CONT-100123/1070

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the input_l2cap_credit function does not check that the metadata corresponding to the user-supplied channel ID actually exists, which can lead to the channel variable being set to NULL before a pointer dereferencing operation is performed. The vulnerability has been patched in the "develop" branch of Contiki-NG, and will be included in release 4.9. Users can apply the patch in Contiki-NG pull request #2253 as a workaround until the new package is released. **CVE ID : CVE-2022-41972**		
Vendor: Dataprobe					
Product: iboot-pdu4-n20_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1071

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1072
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1073
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1074

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1075
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1076
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1077

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**		
Product: iboot-pdu4a-n15_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1078
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1079

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1080
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1081
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1082

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3187		
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1083
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1084
Product: iboot-pdu4a-n20_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1085
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1086
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1087

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other device's information. **CVE ID : CVE-2022-3186**		
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1088
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1089
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1090

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			completed by specific users. **CVE ID : CVE-2022-3188**		
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1091
Product: iboot-pdu4sa-n15_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1092
Improper Limitation	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to	https://www.cisa.gov/u	O-DAT-IBOO-100123/1093

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	scert/ics/advisories/icsa-22-263-03	
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1094
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1095

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1096
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1097
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1098

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**		
Product: iboot-pdu4sa-n20_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1099
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1100

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1101
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1102
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1103

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3187		
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1104
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1105
Product: iboot-pdu8a-2n15_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1106
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1107
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1108

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other device's information. **CVE ID : CVE-2022-3186**		
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1109
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1110
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1111

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			completed by specific users. **CVE ID : CVE-2022-3188**		
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1112
Product: iboot-pdu8a-2n20_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1113
Improper Limitation	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to	https://www.cisa.gov/u	O-DAT-IBOO-100123/1114

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	scert/ics/advisories/icsa-22-263-03	
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1115
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1116

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1117
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1118
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1119

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**		
Product: iboot-pdu8a-n15_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1120
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1121

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1122
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1123
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1124

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3187		
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1125
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1126
Product: iboot-pdu8a-n20_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1127
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1128
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1129

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other device's information. **CVE ID : CVE-2022-3186**		
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1130
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1131
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1132

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			completed by specific users. **CVE ID : CVE-2022-3188**		
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1133
Product: iboot-pdu8sa-2n15_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1134
Improper Limitation	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to	https://www.cisa.gov/u	O-DAT-IBOO-100123/1135

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	scert/ics/advisories/icsa-22-263-03	
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1136
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1137

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1138
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1139
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1140

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**		
Product: iboot-pdu8sa-n15_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1141
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1142

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information. **CVE ID : CVE-2022-3186**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1143
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1144
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets.	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1145

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3187		
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users. **CVE ID : CVE-2022-3188**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1146
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1147
Product: iboot-pdu8sa-n20_firmware					
Affected Version(s): * Up to (excluding) 1.42.06162022					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability. **CVE ID : CVE-2022-3183**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1148
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	9.8	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory. **CVE ID : CVE-2022-3184**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1149
Improper Access Control	21-Dec-2022	7.5	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device's main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1150

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			other device's information. **CVE ID : CVE-2022-3186**		
N/A	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device. **CVE ID : CVE-2022-3185**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1151
Improper Authorization	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets. **CVE ID : CVE-2022-3187**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1152
Missing Authentication for Critical Function	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1153

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			completed by specific users. **CVE ID : CVE-2022-3188**		
Server-Side Request Forgery (SSRF)	21-Dec-2022	5.3	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter. **CVE ID : CVE-2022-3189**	https://www.cisa.gov/uscert/ics/advisories/icsa-22-263-03	O-DAT-IBOO-100123/1154
Vendor: Dlink					
Product: dap-2310_firmware					
Affected Version(s): * Up to (including) 2.10rc036					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662	https://www.dlink.com/en/security-bulletin/	O-DLI-DAP--100123/1155

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**		
Product: dap-2330_firmware					
Affected Version(s): * Up to (including) 1.06rc020					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**	https://www.dlink.com/en/security-bulletin/	O-DLI-DAP--100123/1156
Product: dap-2360_firmware					
Affected Version(s): * Up to (including) 2.10rc050					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and	https://www.dlink.com	O-DLI-DAP--100123/1157

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**	/en/security-bulletin/	
Product: dap-2553_firmware					
Affected Version(s): * Up to (including) 3.10rc031					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of	https://www.dlink.com/en/security-bulletin/	O-DLI-DAP--100123/1158

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**		
Product: dap-2660_firmware					
Affected Version(s): * Up to (including) 1.15rc093					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**	https://www.dlink.com/en/security-bulletin/	O-DLI-DAP--100123/1159
Product: dap-2690_firmware					
Affected Version(s): * Up to (including) 3.20rc106					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050	https://www.dlink.com/en/security-bulletin/	O-DLI-DAP--100123/1160

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**		
Product: dap-2695_firmware					
Affected Version(s): * Up to (excluding) 1.20rc119					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after	https://www.dlink.com/en/security-bulletin/	O-DLI-DAP--100123/1161

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			modifying the firmware header. **CVE ID : CVE-2022-38873**		
Affected Version(s): 1.20rc119					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**	https://www.dlink.com/en/security-bulletin/	O-DLI-DAP--100123/1162
Product: dap-3320_firmware					
Affected Version(s): * Up to (excluding) 1.05rc027					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier,	https://www.dlink.com/en/security-bulletin/	O-DLI-DAP--100123/1163

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**		
Affected Version(s): 1.05rc027					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**	https://www.dlink.com/en/security-bulletin/	O-DLI-DAP--100123/1164
Product: dap-3662_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (including) 1.05rc047					
N/A	20-Dec-2022	7.5	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header. **CVE ID : CVE-2022-38873**	https://www.dlink.com/en/security-bulletin/	O-DLI-DAP--100123/1165
Product: dir-846_firmware					
Affected Version(s): 100a43					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	23-Dec-2022	9.9	D-Link DIR-846 A1_FW100A43 was discovered to contain a command injection vulnerability via the lan(0)_dhcps_staticlist parameter in the SetIpMacBindSettings function. **CVE ID : CVE-2022-46641**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--100123/1166
Improper Neutralization of	23-Dec-2022	9.9	D-Link DIR-846 A1_FW100A43 was discovered to contain a	https://www.dlink.com	O-DLI-DIR--100123/1167

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Special Elements used in a Command ('Command Injection')			command injection vulnerability via the auto_upgrade_hour parameter in the SetAutoUpgradeInfo function. **CVE ID : CVE-2022-46642**	/en/security-bulletin/	
Product: dir-869ax_firmware					
Affected Version(s): fw102b15					
Incorrect Authorization	20-Dec-2022	7.5	D-Link DIR-869 DIR869Ax_FW102B15 is vulnerable to Authentication Bypass via phpcgi. **CVE ID : CVE-2022-46076**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--100123/1168
Product: dir-869_firmware					
Affected Version(s): fw102b15					
Incorrect Authorization	20-Dec-2022	7.5	D-Link DIR-869 DIR869Ax_FW102B15 is vulnerable to Authentication Bypass via phpcgi. **CVE ID : CVE-2022-46076**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--100123/1169
Vendor: Google					
Product: android					
Affected Version(s): -					
N/A	16-Dec-2022	9.8	Product: AndroidVersions: Android kernelAndroid ID: A-235292841References: N/A **CVE ID : CVE-2022-42529**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1170

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	22-Dec-2022	8.8	An attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1. **CVE ID : CVE-2022-1529**	https://bugzilla.mozilla.org/show_bug.cgi?id=1770048, https://www.mozilla.org/security/advisories/mfsa2022-19/	O-GOO-ANDR-100123/1171
Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	22-Dec-2022	8.8	If an attacker was able to corrupt the methods of an Array object in JavaScript via prototype pollution, they could have achieved execution of attacker-controlled JavaScript code in a privileged context. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1. **CVE ID : CVE-2022-1802**	https://bugzilla.mozilla.org/show_bug.cgi?id=1770137, https://www.mozilla.org/security/advisories/mfsa2022-19/	O-GOO-ANDR-100123/1172
Out-of-bounds Write	16-Dec-2022	8.8	In the Pixel cellular firmware, there is a possible out of bounds write due to a missing bounds check. This	https://source.android.com/security/bulletin/pi	O-GOO-ANDR-100123/1173

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			could lead to remote code execution with LTE authentication needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238914868References: N/A **CVE ID : CVE-2022-20607**	xel/2022-12-01	
Cleartext Transmission of Sensitive Information	22-Dec-2022	8.8	When clicking on a tel: link, USSD codes, specified after a <code>*</code> character, would be included in the phone number. On certain phones, or on certain carriers, if the number was dialed this could perform actions on a user's account, similar to a cross-site request forgery attack. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 97. **CVE ID : CVE-2022-22758**	https://bugzilla.mozilla.org/show_bug.cgi?id=1728742, https://www.mozilla.org/security/advisories/mfsa2022-04/	O-GOO-ANDR-100123/1174
Out-of-bounds Read	16-Dec-2022	8.8	In cellular modem firmware, there is a possible out of bounds read due to a missing bounds check. This could lead to remote	https://source.android.com/security/bulletin/pi	O-GOO-ANDR-100123/1175

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			code execution with LTE authentication needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-240462530References: N/A **CVE ID : CVE-2022-20610**	xel/2022-12-01	
Improper Input Validation	16-Dec-2022	7.8	In valid_out_of_special_sec_dram_addr of drm_access_control.c, there is a possible EoP due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238716781References: N/A **CVE ID : CVE-2022-20585**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1176
Use After Free	16-Dec-2022	7.8	In TBD of aud_hal_tunnel.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1177

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-222162870References: N/A **CVE ID : CVE-2022-20561**		
Improper Input Validation	16-Dec-2022	7.8	In valid_out_of_special_sec_dram_addr of drm_access_control.c, there is a possible EoP due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238718854References: N/A **CVE ID : CVE-2022-20586**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1178
Improper Input Validation	16-Dec-2022	7.8	In ppmp_validate_wsm of drm_fw.c, there is a possible EoP due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1179

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android kernelAndroid ID: A-238720411References: N/A **CVE ID : CVE-2022-20587**		
Improper Input Validation	16-Dec-2022	7.8	In page_number of shared_mem.c, there is a possible code execution in secure world due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238366009References: N/A **CVE ID : CVE-2022-20584**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1180
Use After Free	16-Dec-2022	7.8	In l2cap_chan_put of l2cap_core, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1181

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			165329981References: Upstream kernel **CVE ID : CVE-2022-20566**		
Integer Overflow or Wraparound	16-Dec-2022	7.8	In ppmpu_set of ppmpu.c, there is a possible EoP due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243480506References: N/A **CVE ID : CVE-2022-20597**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1182
Use After Free	16-Dec-2022	7.8	In (TBD) of (TBD), there is a possible way to corrupt kernel memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-220738351References: Upstream kernel **CVE ID : CVE-2022-20568**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1183

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	16-Dec-2022	7.8	In sec_media_protect of media.c, there is a possible EoP due to an integer overflow. This could lead to local escalation of privilege of secure mode MFC Core with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242357514References: N/A **CVE ID : CVE-2022-20598**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1184
Out-of-bounds Write	16-Dec-2022	7.8	In ppmp_unprotect_mfcfw_buf of drm_fw.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-233645166References: N/A **CVE ID : CVE-2022-20582**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1185

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Dec-2022	7.8	In TBD of TBD, there is a possible out of bounds write due to memory corruption. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239847859References: N/A **CVE ID : CVE-2022-20600**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1186
Improper Input Validation	16-Dec-2022	7.8	In trusty_ffa_mem_reclaim of shared-mem-smcall.c, there is a possible privilege escalation due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-237838301References: N/A **CVE ID : CVE-2022-42534**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1187
Allocation of Resources	16-Dec-2022	7.8	In mmu_map_for_fw of gs_ldfw_load.c, there is a possible mitigation	https://source.android.com/security	O-GOO-ANDR-100123/1188

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Without Limits or Throttling			bypass due to Permissive Memory Allocation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-231500967References: N/A **CVE ID : CVE-2022-42531**	/bulletin/pixel/2022-12-01	
N/A	16-Dec-2022	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-212623833References: N/A **CVE ID : CVE-2022-20560**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1189
N/A	16-Dec-2022	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-204541506References: N/A **CVE ID : CVE-2022-20601**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1190
N/A	16-Dec-2022	7.5	Product: AndroidVersions: Android kernelAndroid ID: A-211081867References: N/A **CVE ID : CVE-2022-20602**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1191

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Dec-2022	7.5	In SAECOMM_CopyBufferBytes of SAECOMM_Utility.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-231722405References: N/A **CVE ID : CVE-2022-20605**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1192
Out-of-bounds Read	16-Dec-2022	7.5	In sms_GetTpUdlIe of sms_PduCodec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243401445References: N/A **CVE ID : CVE-2022-42524**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1193

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	16-Dec-2022	7.5	In cd_SsParseMsg of cd_SsCodec.c, there is a possible crash due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-244448906References: N/A **CVE ID : CVE-2022-42527**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1194
Out-of-bounds Write	16-Dec-2022	7.2	In SetDecompContextDb of RohcDeCompContextOfRbId.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-219265339References: N/A **CVE ID : CVE-2022-20603**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1195

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Dec-2022	6.7	In verity_target of dm-verity-target.c, there is a possible way to modify read-only files due to a missing permission check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-234475629References: Upstream kernel **CVE ID : CVE-2022-20572**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1196
Out-of-bounds Write	16-Dec-2022	6.7	In ProtocolMiscBuilder::BuildSetSignalReportCriteria of protocolmiscbuilder.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241232492References: N/A **CVE ID : CVE-2022-42505**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1197

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Dec-2022	6.7	In CallDialReqData::encodeCallNumber of callreqdata.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241232209References: N/A **CVE ID : CVE-2022-42504**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1198
Out-of-bounds Write	16-Dec-2022	6.7	In externalOnRequest of rilapplication.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239701761References: N/A **CVE ID : CVE-2022-20576**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1199

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Dec-2022	6.7	In OemSimAuthRequest::encode of wlandata.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241762281References: N/A **CVE ID : CVE-2022-20577**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1200
Out-of-bounds Write	16-Dec-2022	6.7	In RadioImpl::setGsmBroadcastConfig of ril_service_legacy.cpp, there is a possible stack clash leading to memory corruption. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243509749References: N/A **CVE ID : CVE-2022-20578**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1201

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Dec-2022	6.7	In RadioImpl::setCdmaBroadcastConfig of ril_service_legacy.cpp, there is a possible stack clash leading to memory corruption. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243510139References: N/A **CVE ID : CVE-2022-20579**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1202
Out-of-bounds Write	16-Dec-2022	6.7	In ufdt_do_one_fixup of ufdt_overlay.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243629453References: N/A **CVE ID : CVE-2022-20580**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1203
N/A	16-Dec-2022	6.7	In the Pixel camera driver, there is a possible use after free	https://source.android.com/security	O-GOO-ANDR-100123/1204

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			due to a logic error in the code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-245916120References: N/A **CVE ID : CVE-2022-20581**	/bulletin/pixel/2022-12-01	
Out-of-bounds Write	16-Dec-2022	6.7	In ProtocolMiscBuilder::BuildSetLinkCapaReport Criteria of protocolmiscbuilder.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241231983References: N/A **CVE ID : CVE-2022-42503**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1205
Out-of-bounds Write	16-Dec-2022	6.7	In ppmp_unprotect_mfcfw_buf of drm_fw.c, there is a possible out of bounds write due to	https://source.android.com/security/bulletin/pi	O-GOO-ANDR-100123/1206

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			improper input validation. This could lead to local escalation of privilege in S-EL1 with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-234859169References: N/A **CVE ID : CVE-2022-20583**	xel/2022-12-01	
Out-of-bounds Write	16-Dec-2022	6.7	In HexString2Value of util.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241231403References: N/A **CVE ID : CVE-2022-42501**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1207
Out-of-bounds Write	16-Dec-2022	6.7	In FacilityLock::Parse of simdata.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1208

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241231970References: N/A **CVE ID : CVE-2022-42502**		
N/A	16-Dec-2022	6.7	In Pixel firmware, there is a possible exposure of sensitive memory due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242332706References: N/A **CVE ID : CVE-2022-20599**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1209
Out-of-bounds Write	16-Dec-2022	6.7	In updateStart of WirelessCharger.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1210

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android kernelAndroid ID: A-239567689References: N/A **CVE ID : CVE-2022-20594**		
Out-of-bounds Write	16-Dec-2022	6.7	In SimUpdatePbEntry::encode of simdata.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241388399References: N/A **CVE ID : CVE-2022-42506**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1211
Out-of-bounds Read	16-Dec-2022	6.7	In TBD of ufdt_convert, there is a possible out of bounds read due to memory corruption. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242067561References: N/A	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1212

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20563		
Out-of-bounds Write	16-Dec-2022	6.7	In ProtocolSimBuilder::BuildSimUpdatePb3gEntry of protocolsimbuilder.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241388774References: N/A **CVE ID : CVE-2022-42507**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1213
Out-of-bounds Write	16-Dec-2022	6.7	In ProtocolCallBuilder::BuildSendUssd of protocolcallbuilder.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241388966References: N/A	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1214

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42508		
Out-of-bounds Write	16-Dec-2022	6.7	In CallDialReqData::encode of callreqdata.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241544307References: N/A **CVE ID : CVE-2022-42509**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1215
Out-of-bounds Write	16-Dec-2022	6.7	In _ufdt_output_strtab_to_fdt of ufdt_convert.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243798789References: N/A	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1216

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20564		
Out-of-bounds Write	16-Dec-2022	6.7	In EmbmsSessionData::encode of embmsdata.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241762712References: N/A **CVE ID : CVE-2022-42511**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1217
Out-of-bounds Write	16-Dec-2022	6.7	In fillSetupDataCallInfo_V1_6 of ril_service_1_6.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243376893References: N/A	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1218

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42523		
Out-of-bounds Write	16-Dec-2022	6.7	In ProtocolEmbmsBuilder::BuildSetSession of protocolembmsbuilder.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241763204References: N/A **CVE ID : CVE-2022-42513**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1219
Out-of-bounds Write	16-Dec-2022	6.7	In BroadcastSmsConfigsRequestData::encode of smsdata.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242536278References: N/A	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1220

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42518		
Out-of-bounds Write	16-Dec-2022	6.7	In CdmaBroadcastSmsConfigsRequestData::encode of cdmasmsdata.cpp, there is a possible stack clash leading to memory corruption. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242540694References: N/A **CVE ID : CVE-2022-42519**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1221
Use After Free	16-Dec-2022	6.7	In ServiceInterface::HandleRequest of serviceinterface.cpp, there is a possible use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242994270References: N/A	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1222

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-42520		
Out-of-bounds Read	16-Dec-2022	6.7	In StringsRequestData::encode of requestdata.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241762656References: N/A **CVE ID : CVE-2022-42510**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1223
Improper Input Validation	16-Dec-2022	6.7	In thermal_cooling_device_stats_update of thermal_sysfs.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1224

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			229258234References: N/A **CVE ID : CVE-2022-20569**		
Out-of-bounds Write	16-Dec-2022	6.7	In fillSetupDataCallInfo_V1_6 of ril_service_1_6.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243509750References: N/A **CVE ID : CVE-2022-42525**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1225
Out-of-bounds Write	16-Dec-2022	6.7	In ConvertUtf8ToUcs2 of radio_hal_utils.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1226

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			243509880References: N/A **CVE ID : CVE-2022-42526**		
Use After Free	16-Dec-2022	6.7	In extract_metadata of dm-android-verity.c, there is a possible way to corrupt kernel memory due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-234030265References: Upstream kernel **CVE ID : CVE-2022-20571**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1227
Improper Check for Unusual or Exceptional Conditions	16-Dec-2022	6.7	In sysmmu_map of sysmmu.c, there is a possible EoP due to a precondition check failure. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238785915References: N/A	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1228

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20588		
Out-of-bounds Write	16-Dec-2022	6.7	In sendChunk of WirelessCharger.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239700400References: N/A **CVE ID : CVE-2022-20596**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1229
Out-of-bounds Write	16-Dec-2022	6.7	In encode of wlandata.cpp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243130019References: N/A **CVE ID : CVE-2022-42521**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1230
Concurrent Execution	16-Dec-2022	6.4	In pppol2tp_create of l2tp_ppp.c, there is a	https://source.android.c	O-GOO-ANDR-100123/1231

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-186777253References: Upstream kernel **CVE ID : CVE-2022-20567**	om/security/bulletin/pixel/2022-12-01	
URL Redirection to Untrusted Site ('Open Redirect')	22-Dec-2022	6.1	Using the <code>S.browser_fallback_url parameter</code> parameter, an attacker could redirect a user to a URL and cause SameSite=Strict cookies to be sent. *This issue only affects Firefox for Android. Other operating systems are not affected.*. This vulnerability affects Firefox < 107. **CVE ID : CVE-2022-45413**	https://bugzilla.mozilla.org/show_bug.cgi?id=1791201, https://www.mozilla.org/security/advisories/mfsa2022-47/	O-GOO-ANDR-100123/1232
URL Redirection to Untrusted Site ('Open Redirect')	22-Dec-2022	6.1	When closed or sent to the background, Firefox for Android would not properly record and persist HSTS settings. *Note: This issue only affected Firefox for Android. Other operating	https://bugzilla.mozilla.org/show_bug.cgi?id=1757138, https://www.mozilla.org/security/a	O-GOO-ANDR-100123/1233

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			systems are unaffected.*. This vulnerability affects Firefox < 100. **CVE ID : CVE-2022-29910**	dvisories/mfsa2022-16/	
N/A	16-Dec-2022	5.5	In ppmpu_set of ppmpu.c, there is a possible information disclosure due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238939706References: N/A **CVE ID : CVE-2022-20591**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1234
Improper Input Validation	16-Dec-2022	5.5	In valid_va_sec_mfc_check of drm_access_control.c, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1235

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			ID: A-238932493References: N/A **CVE ID : CVE-2022-20590**		
N/A	16-Dec-2022	5.5	Product: AndroidVersions: Android kernelAndroid ID: A-230660904References: N/A **CVE ID : CVE-2022-20570**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1236
Out-of-bounds Read	16-Dec-2022	5.5	In SAECOMM_SetDcnIdForPlmn of SAECOMM_DbManagement.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure from a single device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-230463606References: N/A **CVE ID : CVE-2022-20604**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1237
Out-of-bounds Read	16-Dec-2022	5.5	In read_ppmpu_info of drm_fw.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1238

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-237585040References: N/A **CVE ID : CVE-2022-20575**		
Improper Input Validation	16-Dec-2022	5.5	In sec_sysmmu_info of drm_fw.c, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-237582191References: N/A **CVE ID : CVE-2022-20574**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1239
Improper Input Validation	16-Dec-2022	5.5	In ppmp_validate_secbuf of drm_fw.c, there is a possible information disclosure due to improper input validation. This could lead to local information disclosure	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1240

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238976908References: N/A **CVE ID : CVE-2022-20592**		
Out-of-bounds Read	16-Dec-2022	5.5	In Pixel cellular firmware, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239239246References: N/A **CVE ID : CVE-2022-20608**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1241
Out-of-bounds Read	16-Dec-2022	5.5	In Pixel cellular firmware, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1242

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239240808References: N/A **CVE ID : CVE-2022-20609**		
Out-of-bounds Read	16-Dec-2022	4.9	In SAEMM_MiningCodecTableWithMsgIE of SAEMM_RadioMessageCodec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-233230674References: N/A **CVE ID : CVE-2022-20606**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1243
Out-of-bounds Read	16-Dec-2022	4.4	In ProtocolImsBuilder::BuildSetConfig of protocolimsbuilder.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1244

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241763298References: N/A **CVE ID : CVE-2022-42514**		
Out-of-bounds Read	16-Dec-2022	4.4	In MiscService::DoOemSetRtpPktlossThreshold of miscservice.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241763503References: N/A **CVE ID : CVE-2022-42515**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1245
Out-of-bounds Read	16-Dec-2022	4.4	In ProtocolSimBuilderLegacy::BuildSimGetGbaAuth of protocolsimbuilderlegacy.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1246

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241763577References: N/A **CVE ID : CVE-2022-42516**		
Out-of-bounds Read	16-Dec-2022	4.4	In MiscService::DoOemSetTcsFci of miscservice.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241763682References: N/A **CVE ID : CVE-2022-42517**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1247
Out-of-bounds Read	16-Dec-2022	4.4	In getWpcAuthChallengeResponse of WirelessCharger.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1248

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239700137References: N/A **CVE ID : CVE-2022-20595**		
Improper Input Validation	16-Dec-2022	4.4	In valid_va_secbuf_check of drm_access_control.c, there is a possible ID due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238841928References: N/A **CVE ID : CVE-2022-20589**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1249
Out-of-bounds Read	16-Dec-2022	4.4	In pop_descriptor_string of BufferDescriptor.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1250

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android kernelAndroid ID: A-239415809References: N/A **CVE ID : CVE-2022-20593**		
Out-of-bounds Read	16-Dec-2022	4.4	In DoSetCarrierConfig of miscservice.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243130038References: N/A **CVE ID : CVE-2022-42522**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1251
Out-of-bounds Read	16-Dec-2022	4.4	In Pixel firmware, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1252

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			242331893References: N/A **CVE ID : CVE-2022-42530**		
Out-of-bounds Read	16-Dec-2022	4.4	In Pixel firmware, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242332610References: N/A **CVE ID : CVE-2022-42532**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1253
Out-of-bounds Read	16-Dec-2022	4.4	In fdt_path_offset_namelen of fdt_ro.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-249998113References: N/A **CVE ID : CVE-2022-42543**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1254

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Dec-2022	4.4	In VsimOperationDataExt::encode of vsimdata.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241763050References: N/A **CVE ID : CVE-2022-42512**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1255
N/A	22-Dec-2022	4.3	Under certain circumstances, a JavaScript alert (or prompt) could have been shown while another website was displayed underneath it. This could have been abused to trick the user. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 97. **CVE ID : CVE-2022-22762**	https://bugzilla.mozilla.org/show_bug.cgi?id=1743931, https://www.mozilla.org/security/advisories/mfsa2022-04/	O-GOO-ANDR-100123/1256
Exposure of Resource	16-Dec-2022	3.3	In various functions of ap_input_processor.c, there is a possible way to record audio during	https://source.android.com/security/bulletin/pi	O-GOO-ANDR-100123/1257

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
to Wrong Sphere			a phone call due to a logic error in the code. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-231630423References: N/A **CVE ID : CVE-2022-20562**	xel/2022-12-01	
Affected Version(s): 13.0					
Missing Authorization	16-Dec-2022	7.8	In onCreate of WifiDppConfiguratorActivity.java, there is a possible way for a guest user to add a WiFi configuration due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-224772890 **CVE ID : CVE-2022-20503**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1258
N/A	16-Dec-2022	7.8	In Multiple Locations, there is a possibility to launch arbitrary protected activities due to a confused deputy.	https://source.android.com/security/bulletin/pi	O-GOO-ANDR-100123/1259

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242845514 **CVE ID : CVE-2022-20550**	xel/2022-12-01	
Missing Authorization	16-Dec-2022	7.8	In onCreate of WifiDialogActivity.java, there is a missing permission check. This could lead to local escalation of privilege from a guest user with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-226133034 **CVE ID : CVE-2022-20506**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1260
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Dec-2022	7.8	In onMulticastListUpdateNotificationReceived of UwbEventManager.java, there is a possible arbitrary code execution due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1261

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246649179 **CVE ID : CVE-2022-20507**		
Missing Authorization	16-Dec-2022	7.8	In onAttach of ConfigureWifiSettings.java, there is a possible way for a guest user to change WiFi settings due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-218679614 **CVE ID : CVE-2022-20508**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1262
Improper Input Validation	16-Dec-2022	7.8	In getView of AddAppNetworksFragment.java, there is a possible way to mislead the user about network add requests due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1263

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-224545390 **CVE ID : CVE-2022-42544**		
Out-of-bounds Write	16-Dec-2022	7.8	In setParameter of EqualizerEffect.cpp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-240919398 **CVE ID : CVE-2022-20548**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1264
Improper Restriction of Rendered UI Layers or Frames	16-Dec-2022	7.8	In onCreate of various files, there is a possible tapjacking/overlay attack. This could lead to local escalation of privilege or denial of server with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-227203202 **CVE ID : CVE-2022-20520**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1265
Improper Input Validation	16-Dec-2022	7.8	In navigateUpTo of Task.java, there is a possible way to launch	https://source.android.com/security	O-GOO-ANDR-100123/1266

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			an intent handler with a mismatched intent due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-238602879 **CVE ID : CVE-2022-20512**	/bulletin/pixel/2022-12-01	
N/A	16-Dec-2022	7.8	In multiple functions of AdapterService.java, there is a possible way to manipulate Bluetooth state due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-240301753 **CVE ID : CVE-2022-20547**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1267
Missing Authorization	16-Dec-2022	7.8	In getSlice of ProviderModelSlice.java, there is a missing permission check. This could lead to local escalation of privilege from the guest user with no additional	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1268

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-227470877 **CVE ID : CVE-2022-20522**		
Use After Free	16-Dec-2022	7.8	In SurfaceFlinger::doDump of SurfaceFlinger.cpp, there is possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-237291506 **CVE ID : CVE-2022-20540**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1269
Use After Free	16-Dec-2022	7.8	In compose of Vibrator.cpp, there is a possible arbitrary code execution due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1270

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-228523213 **CVE ID : CVE-2022-20524**		
Integer Overflow or Wraparound	16-Dec-2022	7.5	In rw_t3t_act_handle_check_ndef_rsp of rw_t3t.cc, there is a possible out of bounds read due to an integer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-224002331 **CVE ID : CVE-2022-20516**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1271
Improper Input Validation	16-Dec-2022	7.5	In bindArtworkAndColors of MediaControlPanel.java, there is a possible way to crash the phone due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-239368697	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1272

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20545		
Missing Authorization	16-Dec-2022	6.7	In multiple locations of DreamManagerService.java, there is a missing permission check. This could lead to local escalation of privilege and dismissal of system dialogs with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-225878553 **CVE ID : CVE-2022-20504**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1273
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Dec-2022	6.7	In openFile of CallLogProvider.java, there is a possible permission bypass due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitationProduct: AndroidVersions: Android-13Android ID: A-225981754 **CVE ID : CVE-2022-20505**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1274
Use After Free	16-Dec-2022	6.7	In removeEventHubDevice of InputDevice.cpp, there is a possible OOB	https://source.android.com/security/bulletin/pi	O-GOO-ANDR-100123/1275

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			read due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-245770596 **CVE ID : CVE-2022-20554**	xel/2022-12-01	
Out-of-bounds Read	16-Dec-2022	6.7	In MessageQueueBase of MessageQueueBase.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-247092734 **CVE ID : CVE-2022-20557**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1276
Out-of-bounds Write	16-Dec-2022	6.7	In phNxpNciHal_core_initialized of phNxpNciHal.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1277

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-231445184 **CVE ID : CVE-2022-42542**		
Use After Free	16-Dec-2022	6.7	In acquireFabricatedOverlayIterator, nextFabricatedOverlayInfos, and releaseFabricatedOverlayIterator of Idmap2Service.cpp, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-245727875 **CVE ID : CVE-2022-20514**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1278
Out-of-bounds Write	16-Dec-2022	6.7	In mapGrantorDescr of MessageQueueBase.h, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1279

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-13Android ID: A-244713317 **CVE ID : CVE-2022-20509**		
Out-of-bounds Write	16-Dec-2022	6.7	In parameterToHal of Effect.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the audio server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-237291425 **CVE ID : CVE-2022-20539**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1280
Out-of-bounds Write	16-Dec-2022	6.7	In getCurrentConfigImpl of Effect.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-240266798 **CVE ID : CVE-2022-20546**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1281

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Dec-2022	6.7	In authToken2AidlVec of KeyMintUtils.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-242702451 **CVE ID : CVE-2022-20549**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1282
Improper Restriction of Rendered UI Layers or Frames	16-Dec-2022	6.5	In onCreate of LogAccessDialogActivity.java, there is a possible way to bypass a permission check due to a tapjacking/overlay attack. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-244155265 **CVE ID : CVE-2022-20553**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1283
Missing Authorization	16-Dec-2022	5.5	In getNearbyNotificationStreamingPolicy of DevicePolicyManagerService.java, there is a possible way to learn	https://source.android.com/security/bulletin/pi	O-GOO-ANDR-100123/1284

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			about the notification streaming policy of other users due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-235822336 **CVE ID : CVE-2022-20510**	xel/2022-12-01	
Incorrect Default Permissions	16-Dec-2022	5.5	In getNearbyAppStreamingPolicy of DevicePolicyManagerService.java, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-235821829 **CVE ID : CVE-2022-20511**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1285
Use of a Broken or Risky Cryptographic Algorithm	16-Dec-2022	5.5	In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1286

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-244569759 **CVE ID : CVE-2022-20513**		
N/A	16-Dec-2022	5.5	In onPreferenceClick of AccountTypePreferenceLoader.java, there is a possible way to retrieve protected files from the Settings app due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-220733496 **CVE ID : CVE-2022-20515**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1287
Externally Controlled Reference to a Resource in Another Sphere	16-Dec-2022	5.5	In multiple locations of NfcService.java, there is a possible disclosure of NFC tags due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1288

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-13Android ID: A-199291025 **CVE ID : CVE-2022-20199**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Dec-2022	5.5	In getMessagesByPhoneNumber of MmsSmsProvider.java, there is a possible access to restricted tables due to SQL injection. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-224769956 **CVE ID : CVE-2022-20517**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1289
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Dec-2022	5.5	In query of MmsSmsProvider.java, there is a possible access to restricted tables due to SQL injection. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1290

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-224770203 **CVE ID : CVE-2022-20518**		
Out-of-bounds Read	16-Dec-2022	5.5	In HalCoreCallback of halcore.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure from the NFC firmware with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-229994861 **CVE ID : CVE-2022-20527**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1291
Use After Free	16-Dec-2022	5.5	In btif_a2dp_sink_command_ready of btif_a2dp_sink.cc, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-243922806	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1292

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20552		
Out-of-bounds Read	16-Dec-2022	5.5	In IncFs_GetFilledRangesStartingFrom of incfs.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-228222508 **CVE ID : CVE-2022-20523**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1293
Observable Discrepancy	16-Dec-2022	5.5	In getSmsRoleHolder of RoleService.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-235601770	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1294

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20538		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Dec-2022	5.5	In a query in MmsSmsProvider.java, there is a possible access to restricted tables due to SQL injection. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-224770183 **CVE ID : CVE-2022-42535**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1295
N/A	16-Dec-2022	5.3	In strings.xml, there is a possible permission bypass due to a misleading string. This could lead to remote information disclosure of call logs with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-231585645 **CVE ID : CVE-2022-20530**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1296
NULL Pointer Dereference	16-Dec-2022	5	In sdpu_find_most_specific_service_uuid of sdp_utils.cc, there is a possible way to crash	https://source.android.com/security/bulletin/pi	O-GOO-ANDR-100123/1297

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Bluetooth due to a missing null check. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-227203684 **CVE ID : CVE-2022-20521**	xel/2022-12-01	
Missing Authorization	16-Dec-2022	4.4	In onOptionsItemSelected of ManageApplications.java, there is a possible bypass of profile owner restrictions due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-238745070 **CVE ID : CVE-2022-20544**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1298
Out-of-bounds Read	16-Dec-2022	4.4	In ufdt_get_node_by_path_len of ufdt_convert.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1299

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246194233 **CVE ID : CVE-2022-20555**		
Out-of-bounds Read	16-Dec-2022	4.2	In phNxpNciHal_ioctl of phNxpNciHal.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-238083126 **CVE ID : CVE-2022-20541**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1300
Missing Authorization	16-Dec-2022	3.3	In onCreate of AddAppNetworksActivity.java, there is a possible way for a guest user to configure WiFi networks due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1301

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Android-13Android ID: A-224772678 **CVE ID : CVE-2022-20519**		
Exposure of Resource to Wrong Sphere	16-Dec-2022	3.3	In enforceVisualVoicemailPackage of PhoneInterfaceManager.java, there is a possible leak of visual voicemail package name due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-229742768 **CVE ID : CVE-2022-20525**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1302
Observable Discrepancy	16-Dec-2022	3.3	In registerLocalOnlyHotspotSoftApCallback of WifiManager.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1303

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-13Android ID: A-233605242 **CVE ID : CVE-2022-20535**		
Out-of-bounds Read	16-Dec-2022	3.3	In findParam of HevcUtils.cpp there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-230172711 **CVE ID : CVE-2022-20528**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1304
Missing Authorization	16-Dec-2022	3.3	In registerBroadcastReceiver of RcsService.java, there is a possible way to change preferred TTY mode due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-235100180	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1305

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20536		
Out-of-bounds Write	16-Dec-2022	3.3	In CanvasContext::draw of CanvasContext.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-229742774 **CVE ID : CVE-2022-20526**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1306
Missing Authorization	16-Dec-2022	3.3	In createDialog of WifiScanModeActivity.java, there is a possible way for a Guest user to enable location-sensitive settings due to a missing permission check. This could lead to local escalation of privilege from the Guest user with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-235601169 **CVE ID : CVE-2022-20537**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1307

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Missing Authorization	16-Dec-2022	3.3	In launchConfigNewNetworkFragment of NetworkProviderSettings.java, there is a possible way for the guest user to add a new WiFi network due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246301667 **CVE ID : CVE-2022-20556**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1308
N/A	16-Dec-2022	3.3	In registerReceivers of DeviceCapabilityListener.java, there is a possible way to change preferred TTY mode due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-236264289 **CVE ID : CVE-2022-20558**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1309

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Observable Discrepancy	16-Dec-2022	3.3	In revokeOwnPermissionsOnKill of PermissionManager.java, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-219739967 **CVE ID : CVE-2022-20559**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1310
Missing Authorization	16-Dec-2022	3.3	In getSlice of WifiSlice.java, there is a possible way to connect a new WiFi network from the guest mode due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-232798363	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1311

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-20533		
Exposure of Resource to Wrong Sphere	16-Dec-2022	2.4	In multiple locations of WifiDialogActivity.java, there is a possible limited lockscreen bypass due to a logic error in the code. This could lead to local escalation of privilege in wifi settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-231583603 **CVE ID : CVE-2022-20529**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1312
Improper Input Validation	16-Dec-2022	2.3	In multiple locations, there is a possible display crash loop due to improper input validation. This could lead to local denial of service with system execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-238178261 **CVE ID : CVE-2022-20543**	https://source.android.com/security/bulletin/pixel/2022-12-01	O-GOO-ANDR-100123/1313
Vendor: Hikvision					
Product: ds-3wf01c-2n\/o_firmware					
Affected Version(s): * Up to (excluding) 1.0.4					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Dec-2022	9.8	The web server of some Hikvision wireless bridge products have an access control vulnerability which can be used to obtain the admin permission. The attacker can exploit the vulnerability by sending crafted messages to the affected devices. **CVE ID : CVE-2022-28173**	https://www.hikvision.com/en/support/cybersecurity/security-advisory/access-control-vulnerability-in-some-hikvision-wireless-bridge-products/	O-HIK-DS-3-100123/1314
Product: ds-3wf0ac-2nt_firmware					
Affected Version(s): * Up to (excluding) 1.1.0					
N/A	19-Dec-2022	9.8	The web server of some Hikvision wireless bridge products have an access control vulnerability which can be used to obtain the admin permission. The attacker can exploit the vulnerability by sending crafted messages to the affected devices. **CVE ID : CVE-2022-28173**	https://www.hikvision.com/en/support/cybersecurity/security-advisory/access-control-vulnerability-in-some-hikvision-wireless-bridge-products/	O-HIK-DS-3-100123/1315
Vendor: Huawei					
Product: emui					
Affected Version(s): 11.0.1					
Out-of-bounds Write	20-Dec-2022	9.8	Fingerprint calibration has a vulnerability of lacking boundary judgment. Successful exploitation of this vulnerability may cause out-of-bounds write.	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyo	O-HUA-EMUI-100123/1316

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46319	s.com/en/docs/security/update/security-bulletins-202212-0000001462975397	
Out-of-bounds Read	20-Dec-2022	9.8	The kernel module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may cause memory overwriting. **CVE ID : CVE-2022-46320**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1317
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Dec-2022	7.5	The backup module has a path traversal vulnerability. Successful exploitation of this vulnerability causes unauthorized access to other system files. **CVE ID : CVE-2022-41591**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1318
Deserialization of	20-Dec-2022	7.5	The system tool has inconsistent serialization and	https://consumer.huawei.com/en/su	O-HUA-EMUI-100123/1319

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			deserialization. Successful exploitation of this vulnerability will cause unauthorized startup of components. **CVE ID : CVE-2022-41596**	pport/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	
N/A	20-Dec-2022	7.5	The system service has a vulnerability that causes incorrect return values. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-41599**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1320
N/A	20-Dec-2022	7.5	The application management module has a vulnerability in permission verification. Successful exploitation of this vulnerability causes unexpected clear of device applications. **CVE ID : CVE-2022-46312**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-	O-HUA-EMUI-100123/1321

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				0000001462975397	
Out-of-bounds Read	20-Dec-2022	7.5	The power consumption module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-46317**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1322
N/A	20-Dec-2022	7.5	The Wi-Fi module has a vulnerability in permission verification. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-46321**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1323
N/A	20-Dec-2022	5.3	The HAware module has a function logic error. Successful exploitation of this vulnerability will affect the account removal function in Settings.	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/do	O-HUA-EMUI-100123/1324

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46318	cs/security/update/security-bulletins-202212-0000001462975397	
Affected Version(s): 12.0.0					
Out-of-bounds Write	20-Dec-2022	9.8	Fingerprint calibration has a vulnerability of lacking boundary judgment. Successful exploitation of this vulnerability may cause out-of-bounds write. **CVE ID : CVE-2022-46319**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1325
Out-of-bounds Read	20-Dec-2022	9.8	The kernel module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may cause memory overwriting. **CVE ID : CVE-2022-46320**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1326

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	20-Dec-2022	9.8	Some smartphones have the out-of-bounds write vulnerability.Successful exploitation of this vulnerability may cause system service exceptions. **CVE ID : CVE-2022-46323**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1327
Out-of-bounds Write	20-Dec-2022	9.8	Some smartphones have the out-of-bounds write vulnerability. Successful exploitation of this vulnerability may cause system service exceptions. **CVE ID : CVE-2022-46324**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1328
Out-of-bounds Write	20-Dec-2022	9.8	Some smartphones have the out-of-bounds write vulnerability.Successful exploitation of this vulnerability may cause system service exceptions. **CVE ID : CVE-2022-46325**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/secu	O-HUA-EMUI-100123/1329

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rity-bulletins-202212-0000001462975397	
Out-of-bounds Write	20-Dec-2022	9.8	Some smartphones have the out-of-bounds write vulnerability. Successful exploitation of this vulnerability may cause system service exceptions. **CVE ID : CVE-2022-46326**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1330
N/A	20-Dec-2022	9.8	Some smartphones have configuration issues. Successful exploitation of this vulnerability may cause privilege escalation, which results in system service exceptions. **CVE ID : CVE-2022-46327**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1331
Improper Limitation of a Pathname to a Restricted	20-Dec-2022	7.5	The backup module has a path traversal vulnerability. Successful exploitation of this vulnerability causes	https://consumer.huawei.com/en/support/bulletin/2022/12/,	O-HUA-EMUI-100123/1332

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			unauthorized access to other system files. **CVE ID : CVE-2022-41591**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	
Deserialization of Untrusted Data	20-Dec-2022	7.5	The system tool has inconsistent serialization and deserialization. Successful exploitation of this vulnerability will cause unauthorized startup of components. **CVE ID : CVE-2022-41596**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1333
N/A	20-Dec-2022	7.5	The system service has a vulnerability that causes incorrect return values. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-41599**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1334

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Dec-2022	7.5	The application management module has a vulnerability in permission verification. Successful exploitation of this vulnerability causes unexpected clear of device applications. **CVE ID : CVE-2022-46312**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1335
Out-of-bounds Read	20-Dec-2022	7.5	The power consumption module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-46317**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1336
N/A	20-Dec-2022	7.5	The Wi-Fi module has a vulnerability in permission verification. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-46321**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/secu	O-HUA-EMUI-100123/1337

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rity-bulletins-202212-0000001462975397	
Out-of-bounds Write	20-Dec-2022	7.5	Some smartphones have the out-of-bounds write vulnerability. Successful exploitation of this vulnerability may cause system service exceptions. **CVE ID : CVE-2022-46322**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1338
Improper Input Validation	20-Dec-2022	7.5	Some smartphones have the input validation vulnerability. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-46328**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1339
N/A	20-Dec-2022	5.3	The HAware module has a function logic error. Successful exploitation of this vulnerability will affect	https://consumer.huawei.com/en/support/bulletin/2022/12/,	O-HUA-EMUI-100123/1340

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the account removal function in Settings. **CVE ID : CVE-2022-46318**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	
Affected Version(s): 12.0.1					
Out-of-bounds Read	20-Dec-2022	9.8	The kernel module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may cause memory overwriting. **CVE ID : CVE-2022-46320**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1341
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Dec-2022	7.5	The backup module has a path traversal vulnerability. Successful exploitation of this vulnerability causes unauthorized access to other system files. **CVE ID : CVE-2022-41591**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1342

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	20-Dec-2022	7.5	The system tool has inconsistent serialization and deserialization. Successful exploitation of this vulnerability will cause unauthorized startup of components. **CVE ID : CVE-2022-41596**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1343
N/A	20-Dec-2022	7.5	The system service has a vulnerability that causes incorrect return values. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-41599**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1344
N/A	20-Dec-2022	7.5	The application management module has a vulnerability in permission verification. Successful exploitation of this vulnerability causes unexpected clear of device applications. **CVE ID : CVE-2022-46312**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/secu	O-HUA-EMUI-100123/1345

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				rity-bulletins-202212-0000001462975397	
Out-of-bounds Read	20-Dec-2022	7.5	The power consumption module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-46317**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1346
N/A	20-Dec-2022	7.5	The Wi-Fi module has a vulnerability in permission verification. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-46321**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-EMUI-100123/1347
N/A	20-Dec-2022	5.3	The HAware module has a function logic error. Successful exploitation of this vulnerability will affect	https://consumer.huawei.com/en/support/bulletin/2022/12/,	O-HUA-EMUI-100123/1348

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the account removal function in Settings. **CVE ID : CVE-2022-46318**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	
Product: harmonyos					
Affected Version(s): * Up to (excluding) 2.0					
Out-of-bounds Write	20-Dec-2022	9.8	Fingerprint calibration has a vulnerability of lacking boundary judgment. Successful exploitation of this vulnerability may cause out-of-bounds write. **CVE ID : CVE-2022-46319**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1349
Out-of-bounds Read	20-Dec-2022	9.8	The kernel module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may cause memory overwriting. **CVE ID : CVE-2022-46320**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-	O-HUA-HARM-100123/1350

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				0000001462975397	
Out-of-bounds Write	20-Dec-2022	9.8	Some smartphones have the out-of-bounds write vulnerability.Successful exploitation of this vulnerability may cause system service exceptions. **CVE ID : CVE-2022-46323**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1351
Out-of-bounds Write	20-Dec-2022	9.8	Some smartphones have the out-of-bounds write vulnerability. Successful exploitation of this vulnerability may cause system service exceptions. **CVE ID : CVE-2022-46324**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1352
Out-of-bounds Write	20-Dec-2022	9.8	Some smartphones have the out-of-bounds write vulnerability.Successful exploitation of this vulnerability may cause system service exceptions.	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/do	O-HUA-HARM-100123/1353

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46325	cs/security/update/security-bulletins-202212-0000001462975397	
Out-of-bounds Write	20-Dec-2022	9.8	Some smartphones have the out-of-bounds write vulnerability. Successful exploitation of this vulnerability may cause system service exceptions. **CVE ID : CVE-2022-46326**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1354
N/A	20-Dec-2022	9.8	Some smartphones have configuration issues. Successful exploitation of this vulnerability may cause privilege escalation, which results in system service exceptions. **CVE ID : CVE-2022-46327**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1355
Use After Free	20-Dec-2022	7.5	The contacts component has a free (undefined) provider vulnerability. Successful	https://device.harmonyos.com/en/docs/security/	O-HUA-HARM-100123/1356

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			exploitation of this vulnerability may affect data integrity. **CVE ID : CVE-2022-46311**	update/security-bulletins-202212-0000001462975397	
Out-of-bounds Write	20-Dec-2022	7.5	Some smartphones have the out-of-bounds write vulnerability. Successful exploitation of this vulnerability may cause system service exceptions. **CVE ID : CVE-2022-46322**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1357
Affected Version(s): * Up to (excluding) 2.1					
Improper Authentication	20-Dec-2022	9.8	A thread security vulnerability exists in the authentication process. Successful exploitation of this vulnerability may affect data integrity, confidentiality, and availability. **CVE ID : CVE-2022-46316**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1358
Deserialization of Untrusted Data	20-Dec-2022	7.5	The system tool has inconsistent serialization and deserialization. Successful exploitation of this vulnerability will cause unauthorized startup of components.	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyo	O-HUA-HARM-100123/1359

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41596	s.com/en/docs/security/update/security-bulletins-202212-0000001462975397	
N/A	20-Dec-2022	7.5	The system service has a vulnerability that causes incorrect return values. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-41599**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1360
N/A	20-Dec-2022	7.5	The application management module has a vulnerability in permission verification. Successful exploitation of this vulnerability causes unexpected clear of device applications. **CVE ID : CVE-2022-46312**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1361
N/A	20-Dec-2022	7.5	The ProfileSDK has defects introduced in the design process.	https://device.harmonyos.com/en/do	O-HUA-HARM-100123/1362

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-46315**	cs/security/update/security-bulletins-202212-0000001462975397	
Out-of-bounds Read	20-Dec-2022	7.5	The power consumption module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-46317**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1363
N/A	20-Dec-2022	7.5	The Wi-Fi module has a vulnerability in permission verification. Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-46321**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1364
Improper Input Validation	20-Dec-2022	7.5	Some smartphones have the input validation vulnerability. Successful exploitation	https://consumer.huawei.com/en/support/bullet	O-HUA-HARM-100123/1365

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-46328**	in/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	
N/A	20-Dec-2022	5.3	The HAware module has a function logic error. Successful exploitation of this vulnerability will affect the account removal function in Settings. **CVE ID : CVE-2022-46318**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1366
Affected Version(s): * Up to (excluding) 3.0.0					
N/A	20-Dec-2022	7.5	The TelephonyProvider module has a vulnerability in obtaining values.Successful exploitation of this vulnerability may affect data confidentiality. **CVE ID : CVE-2022-46310**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1367
N/A	20-Dec-2022	7.5	The IPC module has defects introduced in the design process.	https://device.harmonyos.com/en/do	O-HUA-HARM-100123/1368

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation of this vulnerability may affect system availability. **CVE ID : CVE-2022-46314**	cs/security/update/security-bulletins-202212-0000001462975397	
Improper Authentication	20-Dec-2022	5.3	The sensor privacy module has an authentication vulnerability. Successful exploitation of this vulnerability may cause unavailability of the smartphone's camera and microphone. **CVE ID : CVE-2022-46313**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1369
Affected Version(s): 2.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Dec-2022	7.5	The backup module has a path traversal vulnerability. Successful exploitation of this vulnerability causes unauthorized access to other system files. **CVE ID : CVE-2022-41591**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1370
Affected Version(s): 2.1					
Improper Limitation of a Pathname to a Restricted	20-Dec-2022	7.5	The backup module has a path traversal vulnerability. Successful exploitation of this vulnerability causes	https://consumer.huawei.com/en/support/bulletin/2022/12/,	O-HUA-HARM-100123/1371

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			unauthorized access to other system files. **CVE ID : CVE-2022-41591**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	
Affected Version(s): 3.0.0					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Dec-2022	7.5	The backup module has a path traversal vulnerability. Successful exploitation of this vulnerability causes unauthorized access to other system files. **CVE ID : CVE-2022-41591**	https://consumer.huawei.com/en/support/bulletin/2022/12/, https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1372
Improper Authentication	20-Dec-2022	5.5	Some smartphones have authentication-related (including session management) vulnerabilities as the setup wizard is bypassed. Successful exploitation of this vulnerability affects the smartphone availability. **CVE ID : CVE-2022-41590**	https://device.harmonyos.com/en/docs/security/update/security-bulletins-202212-0000001462975397	O-HUA-HARM-100123/1373
Vendor: IBM					
Product: aix					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): -					
Use of a Broken or Risky Cryptographic Algorithm	20-Dec-2022	7.5	IBM Spectrum Control 5.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 233982. **CVE ID : CVE-2022-38391**	https://www.ibm.com/support/pages/node/6847541, https://exchange.xforce.ibmcloud.com/vulnerabilities/233982	O-IBM-AIX-100123/1374
Improper Input Validation	20-Dec-2022	5.5	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 could allow an authenticated user to lock additional RM authorizations, resulting in a denial of service on displaying or managing these authorizations. IBM X-Force ID: 240034. **CVE ID : CVE-2022-43875**	https://www.ibm.com/support/pages/node/6848881, https://exchange.xforce.ibmcloud.com/vulnerabilities/240034	O-IBM-AIX-100123/1375
Improper Authentication	22-Dec-2022	5.3	IBM Security Verify Governance, Identity Manager 10.0.1 software component could allow an authenticated user to modify or cancel any other user's access request using man-in-the-middle techniques. IBM X-Force ID: 231096. **CVE ID : CVE-2022-35646**	https://exchange.xforce.ibmcloud.com/vulnerabilities/231096, https://www.ibm.com/support/pages/node/6850809	O-IBM-AIX-100123/1376

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	20-Dec-2022	5.3	IBM Financial Transaction Manager 3.2.4 authorization checks are done incorrectly for some HTTP requests which allows getting unauthorized technical information (e.g. event log entries) about the FTM SWIFT system. IBM X-Force ID: 239708. **CVE ID : CVE-2022-43872**	https://www.ibm.com/support/pages/node/6848881, https://exchange.xforce.ibmcloud.com/vulnerabilities/239708	O-IBM-AIX-100123/1377
Affected Version(s): 7.1					
Improper Privilege Management	23-Dec-2022	8.4	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the rm_rlcache_file command to obtain root privileges. IBM X-Force ID: 236690. **CVE ID : CVE-2022-41290**	https://www.ibm.com/support/pages/node/6847917, https://exchange.xforce.ibmcloud.com/vulnerabilities/236690	O-IBM-AIX-100123/1378
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to cause a denial of service. IBM X-Force ID: 235181. **CVE ID : CVE-2022-39164**	https://www.ibm.com/support/pages/node/6847947	O-IBM-AIX-100123/1379
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in CAA to	https://exchange.xforce.ibmcloud.com/vulnerabilities/23518	O-IBM-AIX-100123/1380

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service. IBM X-Force ID: 235183. **CVE ID : CVE-2022-39165**	3, https://www.ibm.com/support/pages/node/6847947	
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 235599. **CVE ID : CVE-2022-40233**	https://exchange.xforce.ibmcloud.com/vulnerabilities/235599, https://www.ibm.com/support/pages/node/6847947	O-IBM-AIX-100123/1381
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX NFS kernel extension to cause a denial of service. IBM X-Force ID: 238640. **CVE ID : CVE-2022-43380**	https://www.ibm.com/support/pages/node/6847947, https://exchange.xforce.ibmcloud.com/vulnerabilities/238640	O-IBM-AIX-100123/1382
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX SMB client to cause a denial of service. IBM X-Force ID: 238639. **CVE ID : CVE-2022-43381**	https://www.ibm.com/support/pages/node/6851443, https://exchange.xforce.ibmcloud.com/vulnerabilities/238639	O-IBM-AIX-100123/1383
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged	https://www.ibm.com/support/page	O-IBM-AIX-100123/1384

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			local user to exploit a vulnerability in the AIX perfstat kernel extension to cause a denial of service. IBM X-Force ID: 239169. **CVE ID : CVE-2022-43848**	s/node/6847947, https://exchange.xforce.ibmcloud.com/vulnerabilities/239169	
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX pfcdd kernel extension to cause a denial of service. IBM X-Force ID: 239170. **CVE ID : CVE-2022-43849**	https://exchange.xforce.ibmcloud.com/vulnerabilities/239170, https://www.ibm.com/support/pages/node/6847947	O-IBM-AIX-100123/1385
N/A	20-Dec-2022	4.4	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a local user with elevated privileges to exploit a vulnerability in the lpd daemon to cause a denial of service. IBM X-Force ID: 238641. **CVE ID : CVE-2022-43382**	https://www.ibm.com/support/pages/node/6848309, https://exchange.xforce.ibmcloud.com/vulnerabilities/238641	O-IBM-AIX-100123/1386
Affected Version(s): 7.2					
Improper Privilege Management	23-Dec-2022	8.4	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the rm_rlcache_file command to obtain root privileges. IBM X-Force ID: 236690.	https://www.ibm.com/support/pages/node/6847917, https://exchange.xforce.ibmcloud.com/vulnerabi	O-IBM-AIX-100123/1387

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-41290	lities/236690	
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to cause a denial of service. IBM X-Force ID: 235181. **CVE ID : CVE-2022-39164**	https://www.ibm.com/support/pages/node/6847947	O-IBM-AIX-100123/1388
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in CAA to cause a denial of service. IBM X-Force ID: 235183. **CVE ID : CVE-2022-39165**	https://exchange.xforce.ibmcloud.com/vulnerabilities/235183, https://www.ibm.com/support/pages/node/6847947	O-IBM-AIX-100123/1389
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 235599. **CVE ID : CVE-2022-40233**	https://exchange.xforce.ibmcloud.com/vulnerabilities/235599, https://www.ibm.com/support/pages/node/6847947	O-IBM-AIX-100123/1390
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX NFS kernel extension to cause a denial of	https://www.ibm.com/support/pages/node/6847947, https://exchange.xforce.ibmcloud.co	O-IBM-AIX-100123/1391

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service. IBM X-Force ID: 238640. **CVE ID : CVE-2022-43380**	m/vulnerabilities/238640	
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX SMB client to cause a denial of service. IBM X-Force ID: 238639. **CVE ID : CVE-2022-43381**	https://www.ibm.com/support/pages/node/6851443, https://exchange.xforce.ibmcloud.com/vulnerabilities/238639	O-IBM-AIX-100123/1392
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX perfstat kernel extension to cause a denial of service. IBM X-Force ID: 239169. **CVE ID : CVE-2022-43848**	https://www.ibm.com/support/pages/node/6847947, https://exchange.xforce.ibmcloud.com/vulnerabilities/239169	O-IBM-AIX-100123/1393
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX pfcdd kernel extension to cause a denial of service. IBM X-Force ID: 239170. **CVE ID : CVE-2022-43849**	https://exchange.xforce.ibmcloud.com/vulnerabilities/239170, https://www.ibm.com/support/pages/node/6847947	O-IBM-AIX-100123/1394
N/A	20-Dec-2022	4.4	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a local user with elevated privileges to exploit a vulnerability	https://www.ibm.com/support/pages/node/6848309,	O-IBM-AIX-100123/1395

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in the lpd daemon to cause a denial of service. IBM X-Force ID: 238641. **CVE ID : CVE-2022-43382**	https://exchange.xforce.ibmcloud.com/vulnerabilities/238641	
Affected Version(s): 7.3					
Improper Privilege Management	23-Dec-2022	8.4	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the rm_rlcache_file command to obtain root privileges. IBM X-Force ID: 236690. **CVE ID : CVE-2022-41290**	https://www.ibm.com/support/pages/node/6847917, https://exchange.xforce.ibmcloud.com/vulnerabilities/236690	O-IBM-AIX-100123/1396
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to cause a denial of service. IBM X-Force ID: 235181. **CVE ID : CVE-2022-39164**	https://www.ibm.com/support/pages/node/6847947	O-IBM-AIX-100123/1397
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in CAA to cause a denial of service. IBM X-Force ID: 235183. **CVE ID : CVE-2022-39165**	https://exchange.xforce.ibmcloud.com/vulnerabilities/235183, https://www.ibm.com/support/pages/node/6847947	O-IBM-AIX-100123/1398
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could	https://exchange.xforce.i	O-IBM-AIX-100123/1399

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			allow a non-privileged local user to exploit a vulnerability in the AIX TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 235599. **CVE ID : CVE-2022-40233**	bmcloud.com/vulnerabilities/235599, https://www.ibm.com/support/pages/node/6847947	
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX NFS kernel extension to cause a denial of service. IBM X-Force ID: 238640. **CVE ID : CVE-2022-43380**	https://www.ibm.com/support/pages/node/6847947, https://exchange.xforce.ibmcloud.com/vulnerabilities/238640	O-IBM-AIX-100123/1400
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX SMB client to cause a denial of service. IBM X-Force ID: 238639. **CVE ID : CVE-2022-43381**	https://www.ibm.com/support/pages/node/6851443, https://exchange.xforce.ibmcloud.com/vulnerabilities/238639	O-IBM-AIX-100123/1401
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX perfstat kernel extension to cause a denial of service. IBM X-Force ID: 239169. **CVE ID : CVE-2022-43848**	https://www.ibm.com/support/pages/node/6847947, https://exchange.xforce.ibmcloud.com/vulnerabilities/239169	O-IBM-AIX-100123/1402

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	23-Dec-2022	6.2	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX pfcdd kernel extension to cause a denial of service. IBM X-Force ID: 239170. **CVE ID : CVE-2022-43849**	https://exchange.xforce.ibmcloud.com/vulnerabilities/239170, https://www.ibm.com/support/pages/node/6847947	O-IBM-AIX-100123/1403
N/A	20-Dec-2022	4.4	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a local user with elevated privileges to exploit a vulnerability in the lpd daemon to cause a denial of service. IBM X-Force ID: 238641. **CVE ID : CVE-2022-43382**	https://www.ibm.com/support/pages/node/6848309, https://exchange.xforce.ibmcloud.com/vulnerabilities/238641	O-IBM-AIX-100123/1404
Product: i					
Affected Version(s): 7.3					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4 and 7.5 could allow an authenticated user to access IBM Navigator for i log files they are authorized to but not while using this interface. The remote authenticated user can bypass the interface checks and download log files by modifying servlet filter. IBM X-Force ID: 239301. **CVE ID : CVE-2022-43857**	https://www.ibm.com/support/pages/node/6850801, https://exchange.xforce.ibmcloud.com/vulnerabilities/239301	O-IBM-I-100123/1405

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to access the file system and download files they are authorized to but not while using this interface. The remote authenticated user can bypass the interface checks by modifying a parameter thereby gaining access to their files through this interface. IBM X-Force ID: 239303. **CVE ID : CVE-2022-43858**	https://www.ibm.com/support/pages/node/6850801, https://exchange.xforce.ibmcloud.com/vulnerabilities/239303	O-IBM-I-100123/1406
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to obtain sensitive information for an object they are authorized to but not while using this interface. By performing a UNION based SQL injection an attacker could see file permissions through this interface. IBM X-Force ID: 239304. **CVE ID : CVE-2022-43859**	https://www.ibm.com/support/pages/node/6850801	O-IBM-I-100123/1407
Improper Neutralization of Special Elements used in an SQL Command	24-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to obtain sensitive information they are authorized to but not while using this interface. By	https://www.ibm.com/support/pages/node/6850801, https://exchange.xforce.ibmcloud.co	O-IBM-I-100123/1408

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			performing an SQL injection an attacker could see user profile attributes through this interface. IBM X-Force ID: 239305. **CVE ID : CVE-2022-43860**	m/vulnerabilities/239305	
Affected Version(s): 7.4					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4 and 7.5 could allow an authenticated user to access IBM Navigator for i log files they are authorized to but not while using this interface. The remote authenticated user can bypass the interface checks and download log files by modifying servlet filter. IBM X-Force ID: 239301. **CVE ID : CVE-2022-43857**	https://www.ibm.com/support/pages/node/6850801, https://exchange.xforce.ibmcloud.com/vulnerabilities/239301	O-IBM-I-100123/1409
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to access the file system and download files they are authorized to but not while using this interface. The remote authenticated user can bypass the interface checks by modifying a parameter thereby gaining access to their files through this interface. IBM X-Force ID: 239303.	https://www.ibm.com/support/pages/node/6850801, https://exchange.xforce.ibmcloud.com/vulnerabilities/239303	O-IBM-I-100123/1410

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-43858		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to obtain sensitive information for an object they are authorized to but not while using this interface. By performing a UNION based SQL injection an attacker could see file permissions through this interface. IBM X-Force ID: 239304. **CVE ID : CVE-2022-43859**	https://www.ibm.com/support/pages/node/6850801	O-IBM-I-100123/1411
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to obtain sensitive information they are authorized to but not while using this interface. By performing an SQL injection an attacker could see user profile attributes through this interface. IBM X-Force ID: 239305. **CVE ID : CVE-2022-43860**	https://www.ibm.com/support/pages/node/6850801, https://exchange.xforce.ibmcloud.com/vulnerabilities/239305	O-IBM-I-100123/1412
Affected Version(s): 7.5					
Improper Limitation of a Pathname to a Restricted	22-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4 and 7.5 could allow an authenticated user to access IBM Navigator for i log files they are authorized to but not	https://www.ibm.com/support/pages/node/6850801, https://exch	O-IBM-I-100123/1413

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			while using this interface. The remote authenticated user can bypass the interface checks and download log files by modifying servlet filter. IBM X-Force ID: 239301. **CVE ID : CVE-2022-43857**	ange.xforce.ibmcloud.com/vulnerabilities/239301	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to access the file system and download files they are authorized to but not while using this interface. The remote authenticated user can bypass the interface checks by modifying a parameter thereby gaining access to their files through this interface. IBM X-Force ID: 239303. **CVE ID : CVE-2022-43858**	https://www.ibm.com/support/pages/node/6850801, https://exchange.xforce.ibmcloud.com/vulnerabilities/239303	O-IBM-I-100123/1414
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to obtain sensitive information for an object they are authorized to but not while using this interface. By performing a UNION based SQL injection an attacker could see file permissions through	https://www.ibm.com/support/pages/node/6850801	O-IBM-I-100123/1415

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			this interface. IBM X-Force ID: 239304. **CVE ID : CVE-2022-43859**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-Dec-2022	4.3	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to obtain sensitive information they are authorized to but not while using this interface. By performing an SQL injection an attacker could see user profile attributes through this interface. IBM X-Force ID: 239305. **CVE ID : CVE-2022-43860**	https://www.ibm.com/support/pages/node/6850801, https://exchange.xforce.ibmcloud.com/vulnerabilities/239305	O-IBM-I-100123/1416
Product: linux_on_zseries					
Affected Version(s): -					
Improper Input Validation	20-Dec-2022	5.5	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 could allow an authenticated user to lock additional RM authorizations, resulting in a denial of service on displaying or managing these authorizations. IBM X-Force ID: 240034. **CVE ID : CVE-2022-43875**	https://www.ibm.com/support/pages/node/6848881, https://exchange.xforce.ibmcloud.com/vulnerabilities/240034	O-IBM-LINU-100123/1417
Incorrect Authorization	20-Dec-2022	5.3	IBM Financial Transaction Manager 3.2.4 authorization checks are done	https://www.ibm.com/support/pages/node/684	O-IBM-LINU-100123/1418

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			incorrectly for some HTTP requests which allows getting unauthorized technical information (e.g. event log entries) about the FTM SWIFT system. IBM X-Force ID: 239708. **CVE ID : CVE-2022-43872**	8881, https://exchange.xforce.ibmcloud.com/vulnerabilities/239708	
Vendor: Juniper					
Product: junos					
Affected Version(s): 22.3					
Improper Input Validation	22-Dec-2022	7.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). If a BGP update message is received over an established BGP session, and that message contains a specific, optional transitive attribute, this session will be torn down with an update message error. This issue cannot propagate beyond an affected system as the processing error occurs as soon as the update is received. This issue is exploitable remotely as	https://kb.juniper.net/JSA70175	O-JUN-JUNO-100123/1419

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			the respective attribute will propagate through unaffected systems and intermediate AS (if any). Continuous receipt of a BGP update containing this attribute will create a sustained Denial of Service (DoS) condition. Since this issue only affects 22.3R1, Juniper strongly encourages customers to move to 22.3R1-S1. Juniper SIRT felt that the need to promptly warn customers about this issue affecting the 22.3R1 versions of Junos OS and Junos OS Evolved warranted an Out of Cycle JSA. This issue affects: Juniper Networks Junos OS version 22.3R1. Juniper Networks Junos OS Evolved version 22.3R1-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 22.3R1. Juniper Networks Junos OS Evolved versions prior to 22.3R1-EVO. **CVE ID : CVE-2022-22184**		
Product: junos_os_evolved					
Affected Version(s): 22.3					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	22-Dec-2022	7.5	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). If a BGP update message is received over an established BGP session, and that message contains a specific, optional transitive attribute, this session will be torn down with an update message error. This issue cannot propagate beyond an affected system as the processing error occurs as soon as the update is received. This issue is exploitable remotely as the respective attribute will propagate through unaffected systems and intermediate AS (if any). Continuous receipt of a BGP update containing this attribute will create a sustained Denial of Service (DoS) condition. Since this issue only affects 22.3R1, Juniper strongly encourages customers to move to 22.3R1-S1. Juniper SIRT felt that the need to	https://kb.juniper.net/JSA70175	O-JUN-JUNO-100123/1420

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			promptly warn customers about this issue affecting the 22.3R1 versions of Junos OS and Junos OS Evolved warranted an Out of Cycle JSA. This issue affects: Juniper Networks Junos OS version 22.3R1. Juniper Networks Junos OS Evolved version 22.3R1-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 22.3R1. Juniper Networks Junos OS Evolved versions prior to 22.3R1-EVO. **CVE ID : CVE-2022-22184**		
Vendor: linaro					
Product: op-tee					
Affected Version(s): * Up to (excluding) 3.20					
Improper Verification of Cryptographic Signature	19-Dec-2022	6.4	An unprotected memory-access operation in optee_os in TrustedFirmware Open Portable Trusted Execution Environment (OP-TEE) before 3.20 allows a physically proximate adversary to bypass signature verification and install malicious trusted applications via electromagnetic fault injections. **CVE ID : CVE-2022-47549**	https://people.linaro.org/~joakim.bech/reports/Breaking_cross-world_isolation_on_ARM_TrustZone_through_EM_faults_coredumps_and_UUID_confusion.pdf	O-LIN-OP-T-100123/1421

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Linux					
Product: linux_kernel					
Affected Version(s): -					
Use of a Broken or Risky Cryptographic Algorithm	22-Dec-2022	7.5	IBM Security Verify Governance, Identity Manager 10.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 225007. **CVE ID : CVE-2022-22461**	https://www.ibm.com/support/pages/node/6850845, https://exchange.xforce.ibmcloud.com/vulnerabilities/225077	O-LIN-LINU-100123/1422
Use of a Broken or Risky Cryptographic Algorithm	20-Dec-2022	7.5	IBM Spectrum Control 5.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 233982. **CVE ID : CVE-2022-38391**	https://www.ibm.com/support/pages/node/6847541, https://exchange.xforce.ibmcloud.com/vulnerabilities/233982	O-LIN-LINU-100123/1423
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-Dec-2022	6.8	IBM Spectrum Scale 5.1 could allow users with permissions to create pod, persistent volume and persistent volume claim to access files and directories outside of the volume, including on the host filesystem. IBM X-Force ID: 235740. **CVE ID : CVE-2022-40607**	https://exchange.xforce.ibmcloud.com/vulnerabilities/235740, https://www.ibm.com/support/pages/node/6848231	O-LIN-LINU-100123/1424
Insufficiently	22-Dec-2022	6.5	IBM Security Verify Governance, Identity	https://exchange.xforce.i	O-LIN-LINU-100123/1425

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			Manager 10.0.1 stores user credentials in plain clear text which can be read by a remote authenticated user. IBM X-Force ID: 225009. **CVE ID : CVE-2022-22458**	bmcloud.com/vulnerabilities/225009, https://www.ibm.com/support/pages/node/6849247	
N/A	22-Dec-2022	6.5	Previously Firefox for macOS and Linux would download temporary files to a user-specific directory in <code>/tmp</code>, but this behavior was changed to download them to <code>/tmp</code> where they could be affected by other local users. This behavior was reverted to the original, user-specific directory. *This bug only affects Firefox for macOS and Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.7 and Thunderbird < 91.7. **CVE ID : CVE-2022-26386**	https://bugzilla.mozilla.org/show_bug.cgi?id=1752396, https://www.mozilla.org/security/advisories/mfsa2022-12/, https://www.mozilla.org/security/advisories/mfsa2022-11/	O-LIN-LINU-100123/1426
N/A	22-Dec-2022	6.5	A malicious website that could create a popup could have resized the popup to overlay the address bar with its own content, resulting in potential user confusion or	https://www.mozilla.org/security/advisories/mfsa2022-24/, https://www.mozilla.org/security/a	O-LIN-LINU-100123/1427

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			spoofing attacks. *This bug only affects Thunderbird for Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11. **CVE ID : CVE-2022-34479**	dvisories/mfsa2022-26/, https://www.mozilla.org/security/advisories/mfsa2022-25/, https://bugzilla.mozilla.org/show_bug.cgi?id=1745595	
Server-Side Request Forgery (SSRF)	16-Dec-2022	6.5	Adobe Campaign version 7.3.1 (and earlier) and 8.3.9 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2022-42343**	https://helpx.adobe.com/security/products/campaign/apsb22-58.html	O-LIN-LINU-100123/1428
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Dec-2022	6.1	IBM Security Verify Governance, Identity Manager 10.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended	https://exchange.xforce.ibmcloud.com/vulnerabilities/225004, https://www.ibm.com/support/page	O-LIN-LINU-100123/1429

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 225004. **CVE ID : CVE-2022-22456**	s/node/6849247	
Improper Input Validation	20-Dec-2022	5.5	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 could allow an authenticated user to lock additional RM authorizations, resulting in a denial of service on displaying or managing these authorizations. IBM X-Force ID: 240034. **CVE ID : CVE-2022-43875**	https://www.ibm.com/support/pages/node/6848881, https://exchange.xforce.ibmcloud.com/vulnerabilities/240034	O-LIN-LINU-100123/1430
Generation of Error Message Containing Sensitive Information	24-Dec-2022	5.3	IBM Security Verify Governance, Identity Manager 10.01 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 224915. **CVE ID : CVE-2022-22449**	https://exchange.xforce.ibmcloud.com/vulnerabilities/224915, https://www.ibm.com/support/pages/node/6849247	O-LIN-LINU-100123/1431
Improper Authentication	22-Dec-2022	5.3	IBM Security Verify Governance, Identity Manager 10.0.1 software component could allow an	https://exchange.xforce.ibmcloud.com/vulnerabilities/23109	O-LIN-LINU-100123/1432

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to modify or cancel any other user's access request using man-in-the-middle techniques. IBM X-Force ID: 231096. **CVE ID : CVE-2022-35646**	6, https://www.ibm.com/support/pages/node/6850809	
Incorrect Authorization	20-Dec-2022	5.3	IBM Financial Transaction Manager 3.2.4 authorization checks are done incorrectly for some HTTP requests which allows getting unauthorized technical information (e.g. event log entries) about the FTM SWIFT system. IBM X-Force ID: 239708. **CVE ID : CVE-2022-43872**	https://www.ibm.com/support/pages/node/6848881, https://exchange.xforce.ibmcloud.com/vulnerabilities/239708	O-LIN-LINU-100123/1433
Cleartext Storage of Sensitive Information	22-Dec-2022	4.4	IBM Security Verify Governance, Identity Manager 10.0.1 stores sensitive information including user credentials in plain clear text which can be read by a local privileged user. IBM X-Force ID: 225007. **CVE ID : CVE-2022-22457**	https://exchange.xforce.ibmcloud.com/vulnerabilities/225007, https://www.ibm.com/support/pages/node/6849247	O-LIN-LINU-100123/1434
Affected Version(s): * Up to (excluding) 6.0.11					
Out-of-bounds Write	18-Dec-2022	7.8	An issue was discovered in the Linux kernel before 6.0.11. Missing validation of the number of channels	https://lore.kernel.org/r/20221123153543.8568-5-	O-LIN-LINU-100123/1435

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			in drivers/net/wireless/microchip/wilc1000/cfg80211.c in the WILC1000 wireless driver can trigger a heap-based buffer overflow when copying the list of operating channels from Wi-Fi management frames. **CVE ID : CVE-2022-47518**	philipturnbull@github.com, https://github.com/torvalds/linux/commit/0cdfa9e6f0915e3d243e2393bfa8a22e12d553b0	
Out-of-bounds Write	18-Dec-2022	7.8	An issue was discovered in the Linux kernel before 6.0.11. Missing validation of IEEE80211_P2P_ATTR_OPER_CHANNEL in drivers/net/wireless/microchip/wilc1000/cfg80211.c in the WILC1000 wireless driver can trigger an out-of-bounds write when parsing the channel list attribute from Wi-Fi management frames. **CVE ID : CVE-2022-47519**	https://lore.kernel.org/r/20221123153543.8568-3-philipturnbull@github.com, https://github.com/torvalds/linux/commit/051ae669e4505abbe05165bebf6be7922de11f41	O-LIN-LINU-100123/1436
Out-of-bounds Write	18-Dec-2022	7.8	An issue was discovered in the Linux kernel before 6.0.11. Missing validation of IEEE80211_P2P_ATTR_CHANNEL_LIST in drivers/net/wireless/microchip/wilc1000/cfg80211.c in the WILC1000 wireless driver can trigger a heap-based buffer	https://github.com/torvalds/linux/commit/f9b62f9843c7b0afdaecabbcebf1dbba18599408, https://lore.kernel.org/r/20221123153543.8568-	O-LIN-LINU-100123/1437

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			overflow when parsing the operating channel attribute from Wi-Fi management frames. **CVE ID : CVE-2022-47521**	4-philipturnbull@github.com	
Out-of-bounds Read	18-Dec-2022	7.1	An issue was discovered in the Linux kernel before 6.0.11. Missing offset validation in drivers/net/wireless/microchip/wilc1000/hif.c in the WILC1000 wireless driver can trigger an out-of-bounds read when parsing a Robust Security Network (RSN) information element from a Netlink packet. **CVE ID : CVE-2022-47520**	https://github.com/torvalds/linux/commit/cd21d99e595ec1d8721e1058dcdd4f1f7de1d793, https://lore.kernel.org/r/20221123153543.8568-2-philipturnbull@github.com	O-LIN-LINU-100123/1438
Affected Version(s): From (including) 5.15 Up to (excluding) 5.18.8					
Out-of-bounds Read	23-Dec-2022	8.1	An issue was discovered in ksmbd in the Linux kernel 5.15 through 5.18 before 5.18.18. fs/ksmbd/smb2pdu.c lacks length validation in the non-padding case in smb2_write. **CVE ID : CVE-2022-47940**	https://github.com/torvalds/linux/commit/158a66b245739e15858de42c0ba60fcf3de9b8e6, https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=158a66b245739e15858de42c0ba60fcf3de9b8e6	O-LIN-LINU-100123/1439

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): From (including) 5.15 Up to (excluding) 5.19.2					
Use After Free	23-Dec-2022	9.8	An issue was discovered in ksmbd in the Linux kernel 5.15 through 5.19 before 5.19.2. fs/ksmbd/smb2pdu.c has a use-after-free and OOPS for SMB2_TREE_DISCONNECT. **CVE ID : CVE-2022-47939**	https://github.com/torvalds/linux/commit/cf6531d98190fa2cf92a6d8bbc8af0a4740a223c, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.2	O-LIN-LINU-100123/1440
Out-of-bounds Write	23-Dec-2022	8.8	An issue was discovered in ksmbd in the Linux kernel 5.15 through 5.19 before 5.19.2. There is a heap-based buffer overflow in set_ntacl_dacl, related to use of SMB2_QUERY_INFO_HE after a malformed SMB2_SET_INFO_HE command. **CVE ID : CVE-2022-47942**	https://github.com/torvalds/linux/commit/8f0541186e9ad1b62accc9519cc2b7a7240272a7, https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=8f0541186e9ad1b62accc9519cc2b7a7240272a7	O-LIN-LINU-100123/1441
Missing Release of Memory after Effective Lifetime	23-Dec-2022	7.5	An issue was discovered in ksmbd in the Linux kernel 5.15 through 5.19 before 5.19.2. fs/ksmbd/smb2pdu.c omits a kfree call in certain smb2_handle_negotiate	https://github.com/torvalds/linux/commit/aa7253c2393f6dcd6a1468b0792f6da76edad917, https://git.kernel.org/cgi	O-LIN-LINU-100123/1442

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			error conditions, aka a memory leak. **CVE ID : CVE-2022-47941**	t/linux/kernel/git/torvalds/linux.git/commit/?id=aa7253c2393f6dcd6a1468b0792f6da76edad917	
Out-of-bounds Read	23-Dec-2022	6.5	An issue was discovered in ksmbd in the Linux kernel 5.15 through 5.19 before 5.19.2. fs/ksmbd/smb2misc.c has an out-of-bounds read and OOPS for SMB2_TREE_CONNECT. **CVE ID : CVE-2022-47938**	https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=824d4f64c20093275f72fc8101394d75ff6a249e, https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.2	O-LIN-LINU-100123/1443
Vendor: Microchip					
Product: bm64_firmware					
Affected Version(s): 1.43					
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM64-100123/1444

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM64-100123/1445
Product: bm70_firmware					
Affected Version(s): 1.43					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM70-100123/1446
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-	O-MIC-BM70-100123/1447

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				in-bluetooth-le	
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM70-100123/1448
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM70-100123/1449
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-	O-MIC-BM70-100123/1450

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				in-bluetooth-le	
Product: bm71_firmware					
Affected Version(s): 1.43					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM71-100123/1451
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM71-100123/1452
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/de	O-MIC-BM71-100123/1453

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				viating-behaviors-in-bluetooth-le	
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM71-100123/1454
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM71-100123/1455
Product: bm77_firmware					
Affected Version(s): 1.43					
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero.	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability	O-MIC-BM77-100123/1456

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46399	-response/deviating-behaviors-in-bluetooth-le	
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM77-100123/1457
Product: bm78_firmware					
Affected Version(s): 1.43					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM78-100123/1458
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is	https://www.microchip.com/en-us/products/wireless-connectivity	O-MIC-BM78-100123/1459

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM78-100123/1460
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM78-100123/1461
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText	https://www.microchip.com/en-us/products/wireless-connectivity/software-	O-MIC-BM78-100123/1462

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before pairing is complete. **CVE ID : CVE-2022-46401**	vulnerability-response/deviating-behaviors-in-bluetooth-le	
Product: bm83_firmware					
Affected Version(s): 1.43					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM83-100123/1463
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM83-100123/1464
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112)	https://www.microchip.com/en-us/products/wireless-	O-MIC-BM83-100123/1465

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	connectivity /software-vulnerability - response/deviating-behaviors-in-bluetooth-le	
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM83-100123/1466
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-BM83-100123/1467
Product: is1870_firmware					
Affected Version(s): 1.43					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC	https://www.microchip.com/en-	O-MIC-IS18-100123/1468

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-IS18-100123/1469
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-IS18-100123/1470
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer	https://www.microchip.com/en-us/products	O-MIC-IS18-100123/1471

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	
Product: is1871_firmware					
Affected Version(s): 1.43					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-IS18-100123/1472
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-IS18-100123/1473
Improper Validation	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43	https://www.microchip.	O-MIC-IS18-100123/1474

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
of Integrity Check Value			(and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-IS18-100123/1475
Product: pic32cx1012bz25048_firmware					
Affected Version(s): -					
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-PIC3-100123/1476

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): 1.43					
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-PIC3-100123/1477
Product: pic_lightblue_explorer_demo_firmware					
Affected Version(s): 4.2_dt100112					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-PIC_-100123/1478
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-	O-MIC-PIC_-100123/1479

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				behaviors-in-bluetooth-le	
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-PIC_-100123/1480
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-PIC_-100123/1481
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-	O-MIC-PIC_-100123/1482

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
				in-bluetooth-le	
Product: rn4678_firmware					
Affected Version(s): 1.43					
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-RN46-100123/1483
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-RN46-100123/1484
Product: rn4870_firmware					
Affected Version(s): 1.43					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages.	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability	O-MIC-RN48-100123/1485

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46403	-response/deviating-behaviors-in-bluetooth-le	
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-RN48-100123/1486
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-RN48-100123/1487
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing.	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-	O-MIC-RN48-100123/1488

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46400	response/deviating-behaviors-in-bluetooth-le	
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-RN48-100123/1489
Product: rn4871_firmware					
Affected Version(s): 1.43					
N/A	19-Dec-2022	8.6	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages. **CVE ID : CVE-2022-46403**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-RN48-100123/1490
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero.	https://www.microchip.com/en-us/products/wireless-connectivity/software-	O-MIC-RN48-100123/1491

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46399	vulnerability-response/deviating-behaviors-in-bluetooth-le	
Improper Validation of Integrity Check Value	19-Dec-2022	6.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values. **CVE ID : CVE-2022-46402**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-RN48-100123/1492
Incorrect Authorization	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing. **CVE ID : CVE-2022-46400**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-RN48-100123/1493
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability	O-MIC-RN48-100123/1494

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			before pairing is complete. **CVE ID : CVE-2022-46401**	-response/deviating-behaviors-in-bluetooth-le	
Product: wbz451_firmware					
Affected Version(s): -					
N/A	19-Dec-2022	5.4	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete. **CVE ID : CVE-2022-46401**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-WBZ4-100123/1495
Affected Version(s): 1.43					
Incorrect Authorization	19-Dec-2022	7.5	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero. **CVE ID : CVE-2022-46399**	https://www.microchip.com/en-us/products/wireless-connectivity/software-vulnerability-response/deviating-behaviors-in-bluetooth-le	O-MIC-WBZ4-100123/1496
Vendor: Microsoft					
Product: windows					
Affected Version(s): -					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-Dec-2022	8.8	The constructed curl command from the "Copy as curl" feature in DevTools was not properly escaped for PowerShell. This could have lead to command injection if pasted into a Powershell prompt. *This bug only affects Thunderbird for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22744**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	O-MIC-WIND-100123/1497
Inadequate Encryption Strength	19-Dec-2022	7.8	In specific scenarios, on Windows the operator credentials may be encrypted in a manner that is not completely machine-dependent. **CVE ID : CVE-2022-38659**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0102049	O-MIC-WIND-100123/1498
Use of a Broken or Risky Cryptographic Algorithm	20-Dec-2022	7.5	IBM Spectrum Control 5.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 233982. **CVE ID : CVE-2022-38391**	https://www.ibm.com/support/pages/node/6847541, https://exchange.xforce.ibmcloud.com/vulnerabilities/233982	O-MIC-WIND-100123/1499
N/A	24-Dec-2022	7.5	BigFix deployments that have installed the	https://support.hcltechs	O-MIC-WIND-100123/1500

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			Notification Service on Windows are susceptible to disclosing SMTP BigFix operator's sensitive data in clear text. Operators who use Notification Service related content from BES Support are at risk of leaving their SMTP sensitive data exposed. **CVE ID : CVE-2022-38658**	w.com/csm?id=kb_article&sysparm_article=KB0102117	
Time-of-check Time-of-use (TOCTOU) Race Condition	22-Dec-2022	7.1	A Time-of-Check Time-of-Use bug existed in the Maintenance (Updater) Service that could be abused to grant Users write access to an arbitrary directory. This could have been used to escalate to SYSTEM access. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6. **CVE ID : CVE-2022-22753**	https://bugzilla.mozilla.org/show_bug.cgi?id=1732435, https://www.mozilla.org/security/advisories/mfsa2022-06/, https://www.mozilla.org/security/advisories/mfsa2022-05/, https://www.mozilla.org/security/advisories/mfsa2022-04/	O-MIC-WIND-100123/1501
N/A	22-Dec-2022	6.5	By generally accepting and passing resource handles across processes, a compromised content process might have confused higher privileged processes to	https://www.mozilla.org/security/advisories/mfsa2022-01/, https://bugzilla.mozilla.org/show_bu	O-MIC-WIND-100123/1502

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			interact with handles that the unprivileged process should not have access to. *This bug only affects Firefox for Windows and MacOS. Other operating systems are unaffected.*. This vulnerability affects Firefox < 96. **CVE ID : CVE-2022-22750**	g.cgi?id=1566608	
Server-Side Request Forgery (SSRF)	16-Dec-2022	6.5	Adobe Campaign version 7.3.1 (and earlier) and 8.3.9 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction. **CVE ID : CVE-2022-42343**	https://helpx.adobe.com/security/products/campaign/apsb22-58.html	O-MIC-WIND-100123/1503
Improper Preservation of Permissions	16-Dec-2022	6	Improper preservation of permissions vulnerability in Trellix Endpoint Agent (xAgent) prior to V35.31.22 on Windows allows a local user with administrator privileges to bypass the product protection to	https://docs.trellix.com/bundle/xagent_35-31-22_rn/page/UUID-73c848e7-6107-fe11-d83d-	O-MIC-WIND-100123/1504

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			uninstall the agent via incorrectly applied permissions in the removal protection functionality. **CVE ID : CVE-2022-4326**	b17bd5b1449c.html	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Dec-2022	5.9	A race condition could have allowed bypassing the fullscreen notification which could have lead to a fullscreen window spoof being unnoticed. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5. **CVE ID : CVE-2022-22746**	https://www.mozilla.org/security/advisories/mfsa2022-02/, https://www.mozilla.org/security/advisories/mfsa2022-01/, https://www.mozilla.org/security/advisories/mfsa2022-03/	O-MIC-WIND-100123/1505
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44498**	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	O-MIC-WIND-100123/1506

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44499**	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	O-MIC-WIND-100123/1507
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44500**	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	O-MIC-WIND-100123/1508
Out-of-bounds Read	16-Dec-2022	5.5	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of	https://helpx.adobe.com/security/products/illustrator/apsb22-60.html	O-MIC-WIND-100123/1509

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2022-44502**		
Cleartext Storage of Sensitive Information	19-Dec-2022	5.5	Sensitive information was stored in plain text in a file that is accessible by a user with a local account in Hybrid Cloud Observability (HCO)/ SolarWinds Platform 2022.4. No other versions are affected **CVE ID : CVE-2022-47512**	https://documentation.solarwinds.com/en/success_center/orionplatform/content/release_notes/solarwinds_platform_2022-4-1_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/CVE-2022-47512	O-MIC-WIND-100123/1510
Improper Authentication	22-Dec-2022	5.3	IBM Security Verify Governance, Identity Manager 10.0.1 software component could allow an authenticated user to modify or cancel any other user's access request using man-in-the-middle techniques.	https://exchange.xforce.ibmcloud.com/vulnerabilities/231096, https://www.ibm.com/support/pages/node/6850809	O-MIC-WIND-100123/1511

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 231096. **CVE ID : CVE-2022-35646**		
Vendor: Netgear					
Product: nighthawk_ax11000_firmware					
Affected Version(s): * Up to (excluding) 1.0.9.90					
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication. **CVE ID : CVE-2022-47208**	https://www.tenable.com/security/research/tra-2022-37	O-NET-NIGH-100123/1512
Product: nighthawk_ax1800_firmware					
Affected Version(s): * Up to (excluding) 1.0.9.90					
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication. **CVE ID : CVE-2022-47208**	https://www.tenable.com/security/research/tra-2022-37	O-NET-NIGH-100123/1513
Product: nighthawk_ax2400_firmware					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Affected Version(s): * Up to (excluding) 1.0.9.90					
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication. **CVE ID : CVE-2022-47208**	https://www.tenable.com/security/research/tra-2022-37	O-NET-NIGH-100123/1514
Product: nighthawk_ax3000_firmware					
Affected Version(s): * Up to (excluding) 1.0.9.90					
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication. **CVE ID : CVE-2022-47208**	https://www.tenable.com/security/research/tra-2022-37	O-NET-NIGH-100123/1515
Product: nighthawk_ax5400_firmware					
Affected Version(s): * Up to (excluding) 1.0.9.90					
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An	https://www.tenable.com/security/research/tra-2022-37	O-NET-NIGH-100123/1516

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication. **CVE ID : CVE-2022-47208**		
Product: nighthawk_ax6000_firmware					
Affected Version(s): * Up to (excluding) 1.0.9.90					
Improper Input Validation	16-Dec-2022	8.8	The "puhttpsniff" service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication. **CVE ID : CVE-2022-47208**	https://www.tenable.com/security/research/tra-2022-37	O-NET-NIGH-100123/1517
Product: rax30_firmware					
Affected Version(s): * Up to (excluding) 1.0.9.90					
Use of Hard-coded Credentials	16-Dec-2022	8.8	A support user exists on the device and appears to be a backdoor for Technical Support staff. The default password for this account is "support" and cannot be changed by a user via any normally accessible means. **CVE ID : CVE-2022-47209**	https://www.tenable.com/security/research/tra-2022-37	O-NET-RAX3-100123/1518

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.8	The default console presented to users over telnet (when enabled) is restricted to a subset of commands. Commands issued at this console, however, appear to be fed directly into a system call or other similar function. This allows any authenticated user to execute arbitrary commands on the device. **CVE ID : CVE-2022-47210**	https://www.tenable.com/security/research/tra-2022-37	O-NET-RAX3-100123/1519
Product: wnr2000_firmware					
Affected Version(s): * Up to (including) 1.2.3.7					
N/A	20-Dec-2022	8.1	An exploitable firmware modification vulnerability was discovered on the Netgear WNR2000v1 router. An attacker can conduct a MITM (Man-in-the-Middle) attack to modify the user-uploaded firmware image and bypass the CRC check, allowing attackers to execute arbitrary code or cause a Denial of Service (DoS). This affects v1.2.3.7 and earlier. **CVE ID : CVE-2022-46423**	https://www.netgear.com/about/security/	O-NET-WNR2-100123/1520
N/A	20-Dec-2022	4.8	An issue in Netgear WNR2000 v1 1.2.3.7 and earlier allows authenticated attackers	https://www.netgear.com/about/security/	O-NET-WNR2-100123/1521

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46422**		
Product: xwn5001_firmware					
Affected Version(s): * Up to (including) 0.4.1.1					
N/A	20-Dec-2022	8.1	An exploitable firmware modification vulnerability was discovered on the Netgear XWN5001 Powerline 500 WiFi Access Point. An attacker can conduct a MITM (Man-in-the-Middle) attack to modify the user-uploaded firmware image and bypass the CRC check, allowing attackers to execute arbitrary code or cause a Denial of Service (DoS). This affects v0.4.1.1 and earlier. **CVE ID : CVE-2022-46424**	https://www.netgear.com/about/security/	O-NET-XWN5-100123/1522
Vendor: Nokia					
Product: fastmile_firmware					
Affected Version(s): 3tg00118abad52					
Use of Hard-coded Credentials	21-Dec-2022	8.4	Nokia Fastmile 3tg00118abad52 devices shipped by Optus are shipped with a default hardcoded admin account of admin:Nq+L5st7o This	N/A	O-NOK-FAST-100123/1523

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			account can be used locally to access the web admin interface. **CVE ID : CVE-2022-36222**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Dec-2022	6.5	Nokia Fastmile 3tg00118abad52 is affected by an authenticated path traversal vulnerability which allows attackers to read any named pipe file on the system. **CVE ID : CVE-2022-36221**	N/A	O-NOK-FAST-100123/1524
Vendor: Oracle					
Product: solaris					
Affected Version(s): -					
Improper Authentication	22-Dec-2022	5.3	IBM Security Verify Governance, Identity Manager 10.0.1 software component could allow an authenticated user to modify or cancel any other user's access request using man-in-the-middle techniques. IBM X-Force ID: 231096. **CVE ID : CVE-2022-35646**	https://exchange.xforce.ibmcloud.com/vulnerabilities/231096, https://www.ibm.com/support/pages/node/6850809	O-ORA-SOLA-100123/1525
Vendor: paxtechnology					
Product: paydroid					
Affected Version(s): 7.1.1_virgo_v04.3.26t1_20210419					
Improper Input Validation	16-Dec-2022	7.8	The systool_server in PAX Technology A930 PayDroid 7.1.1 Virgo V04.4.02 20211201 fails to check for dollar	N/A	O-PAX-PAYD-100123/1526

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			signs or backticks in user supplied commands, leading to to arbitrary command execution as root. **CVE ID : CVE-2022-26582**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Dec-2022	6.8	PAX Technology A930 PayDroid 7.1.1 Virgo V04.4.02 20211201 was discovered to be vulnerable to command injection. **CVE ID : CVE-2022-26580**	N/A	O-PAX-PAYD-100123/1527
Missing Authorization	16-Dec-2022	6.8	The ADB daemon in PAX Technology A930 PayDroid 7.1.1 Virgo V04.4.02 20211201 allows the execution of the systool utility in production mode, allowing unauthenticated attackers to perform privileged actions. **CVE ID : CVE-2022-26581**	N/A	O-PAX-PAYD-100123/1528
Insufficient Verification of Data Authenticity	16-Dec-2022	6	PAX Technology A930 PayDroid 7.1.1 Virgo V04.4.02 20211201 allows root privileged attackers to install an unsigned application by copying the APK to /data/app, setting the appropriate permissions and rebooting the device.	N/A	O-PAX-PAYD-100123/1529

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-26579		
Vendor: Redhat					
Product: enterprise_linux					
Affected Version(s): 8.0					
Out-of-bounds Write	19-Dec-2022	7.1	When rendering certain unicode sequences, grub2's font code doesn't proper validate if the informed glyph's width and height is constrained within bitmap size. As consequence an attacker can craft an input which will lead to a out-of-bounds write into grub2's heap, leading to memory corruption and availability issues. Although complex, arbitrary code execution could not be discarded. **CVE ID : CVE-2022-3775**	N/A	O-RED-ENTE-100123/1530
Vendor: Rockwellautomation					
Product: compactlogix_5370_firmware					
Affected Version(s): From (including) 20 Up to (including) 33					
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS).	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757	O-ROC-COMP-100123/1531

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3157		
Product: compactlogix_5380_firmware					
Affected Version(s): -					
N/A	19-Dec-2022	7.5	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition in Rockwell Automation Logix controllers resulting in a major non-recoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online and continue normal operation. **CVE ID : CVE-2022-3752**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137664	O-ROC-COMP-100123/1532
Product: compactlogix_5480_firmware					
Affected Version(s): * Up to (excluding) 0.0.13					
N/A	19-Dec-2022	7.5	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition in Rockwell Automation Logix controllers resulting in a major non-recoverable fault. If the target device becomes unavailable, a user	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137664	O-ROC-COMP-100123/1533

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			would have to clear the fault and redownload the user project file to bring the device back online and continue normal operation. **CVE ID : CVE-2022-3752**		
Product: compactlogix_5580_firmware					
Affected Version(s): -					
N/A	19-Dec-2022	7.5	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition in Rockwell Automation Logix controllers resulting in a major non-recoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online and continue normal operation. **CVE ID : CVE-2022-3752**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137664	O-ROC-COMP-100123/1534
Product: compact_guardlogix_5370_firmware					
Affected Version(s): From (including) 28 Up to (including) 33					
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757	O-ROC-COMP-100123/1535

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			(MNRF) and a denial-of-service condition (DOS). **CVE ID : CVE-2022-3157**		
Product: compact_guardlogix_5380_firmware					
Affected Version(s): -					
N/A	19-Dec-2022	7.5	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition in Rockwell Automation Logix controllers resulting in a major non-recoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online and continue normal operation. **CVE ID : CVE-2022-3752**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137664	O-ROC-COMP-100123/1536
Affected Version(s): From (including) 28 Up to (including) 33					
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS).	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757	O-ROC-COMP-100123/1537

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-3157		
Product: controllogix_5570_firmware					
Affected Version(s): From (including) 20 Up to (including) 33					
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS). **CVE ID : CVE-2022-3157**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757	O-ROC-CONT-100123/1538
Product: controllogix_5570_redundancy_firmware					
Affected Version(s): From (including) 20 Up to (including) 33					
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS). **CVE ID : CVE-2022-3157**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757	O-ROC-CONT-100123/1539
Product: guardlogix_5570_firmware					
Affected Version(s): From (including) 20 Up to (including) 33					
N/A	16-Dec-2022	7.5	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137757	O-ROC-GUAR-100123/1540

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			service condition (DOS). **CVE ID : CVE-2022-3157**		
Product: guardlogix_5580_firmware					
Affected Version(s): -					
N/A	19-Dec-2022	7.5	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition in Rockwell Automation Logix controllers resulting in a major non-recoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online and continue normal operation. **CVE ID : CVE-2022-3752**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137664	O-ROC-GUAR-100123/1541
Product: micrologix_1100_firmware					
Affected Version(s): -					
Improper Enforcement of Message Integrity During Transmission in a Communication Channel	16-Dec-2022	7.5	Rockwell Automation was made aware that the webservers of the Micrologix 1100 and 1400 controllers contain a vulnerability that may lead to a denial-of-service condition. The security vulnerability could be exploited by an attacker	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137678	O-ROC-MICR-100123/1542

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			with network access to the affected systems by sending TCP packets to webserver and closing it abruptly which would cause a denial-of-service condition for the web server application on the device **CVE ID : CVE-2022-3166**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Rockwell Automation was made aware of a vulnerability by a security researcher from Georgia Institute of Technology that the MicroLogix 1100 and 1400 controllers contain a vulnerability that may give an attacker the ability to accomplish remote code execution. The vulnerability is an unauthenticated stored cross-site scripting vulnerability in the embedded webserver. The payload is transferred to the controller over SNMP and is rendered on the homepage of the embedded website. **CVE ID : CVE-2022-46670**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137679	O-ROC-MICR-100123/1543
Product: micrologix_1400-a_firmware					
Affected Version(s): * Up to (including) 7.000					
Improper Neutralizat	16-Dec-2022	6.1	Rockwell Automation was made aware of a	https://rockwellautomat	O-ROC-MICR-100123/1544

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			vulnerability by a security researcher from Georgia Institute of Technology that the MicroLogix 1100 and 1400 controllers contain a vulnerability that may give an attacker the ability to accomplish remote code execution. The vulnerability is an unauthenticated stored cross-site scripting vulnerability in the embedded webserver. The payload is transferred to the controller over SNMP and is rendered on the homepage of the embedded website. **CVE ID : CVE-2022-46670**	ion.custhelp.com/app/answers/answer_view/a_id/1137679	
Product: micrologix_1400-b_firmware					
Affected Version(s): * Up to (including) 21.007					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Rockwell Automation was made aware of a vulnerability by a security researcher from Georgia Institute of Technology that the MicroLogix 1100 and 1400 controllers contain a vulnerability that may give an attacker the ability to accomplish remote code execution. The vulnerability is an unauthenticated stored cross-site scripting vulnerability in the	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137679	O-ROC-MICR-100123/1545

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			embedded webserver. The payload is transferred to the controller over SNMP and is rendered on the homepage of the embedded website. **CVE ID : CVE-2022-46670**		
Product: micrologix_1400-c_firmware					
Affected Version(s): * Up to (including) 21.007					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Rockwell Automation was made aware of a vulnerability by a security researcher from Georgia Institute of Technology that the MicroLogix 1100 and 1400 controllers contain a vulnerability that may give an attacker the ability to accomplish remote code execution. The vulnerability is an unauthenticated stored cross-site scripting vulnerability in the embedded webserver. The payload is transferred to the controller over SNMP and is rendered on the homepage of the embedded website. **CVE ID : CVE-2022-46670**	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137679	O-ROC-MICR-100123/1546
Product: micrologix_1400_firmware					
Affected Version(s): -					
Improper Enforceme	16-Dec-2022	7.5	Rockwell Automation was made aware that	https://rockwellautomat	O-ROC-MICR-100123/1547

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
nt of Message Integrity During Transmission in a Communication Channel			the webservers of the Micrologix 1100 and 1400 controllers contain a vulnerability that may lead to a denial-of-service condition. The security vulnerability could be exploited by an attacker with network access to the affected systems by sending TCP packets to webserver and closing it abruptly which would cause a denial-of-service condition for the web server application on the device **CVE ID : CVE-2022-3166**	ion.custhelp.com/app/answers/answer_view/a_id/1137678	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Dec-2022	6.1	Rockwell Automation was made aware of a vulnerability by a security researcher from Georgia Institute of Technology that the MicroLogix 1100 and 1400 controllers contain a vulnerability that may give an attacker the ability to accomplish remote code execution. The vulnerability is an unauthenticated stored cross-site scripting vulnerability in the embedded webserver. The payload is transferred to the controller over SNMP and is rendered on the	https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1137679	O-ROC-MICR-100123/1548

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			homepage of the embedded website. **CVE ID : CVE-2022-46670**		
Vendor: Sharp					
Product: bp-30c25t_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-3-100123/1549
Product: bp-30c25y_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-3-100123/1550

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-30c25z_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-3-100123/1551

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-30c25_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-3-100123/1552
Product: bp-30m28t_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-3-100123/1553

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-30m28_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-3-100123/1554

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-30m31t_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-3-100123/1555
Product: bp-30m31_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-3-100123/1556

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-30m35t_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-3-100123/1557

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-30m35_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-3-100123/1558
Product: bp-50c26_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1559

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50c31_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1560

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50c36_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1561
Product: bp-50c45_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1562

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50c55_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1563

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50c65_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1564
Product: bp-50m26_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1565

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50m31_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1566

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50m36_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1567
Product: bp-50m45_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1568

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50m50_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1569

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-50m55_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1570
Product: bp-55c26_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-5-100123/1571

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-60c31_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-6-100123/1572

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-60c36_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-6-100123/1573
Product: bp-60c45_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-6-100123/1574

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70c31_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1575

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70c36_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1576
Product: bp-70c45_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1577

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70c55_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1578

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70c65_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1579
Product: bp-70m31_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1580

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70m36_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1581

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70m45_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1582
Product: bp-70m55_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1583

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70m65_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1584

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: bp-70m75_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1585
Product: bp-70m90_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-BP-7-100123/1586

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-2630n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-2-100123/1587

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-2651_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-2-100123/1588
Product: mx-3050n_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1589

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3050n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1590

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3050v_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1591
Product: mx-3050v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1592

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3051_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1593

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3060n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1594
Product: mx-3060v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1595

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3061s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1596

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3061_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1597
Product: mx-3070n_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1598

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3070n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1599

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3070v_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1600
Product: mx-3070v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1601

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3071s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1602

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3071_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1603
Product: mx-3550n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1604

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3550v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1605

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3551_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1606
Product: mx-3560n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1607

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3560v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1608

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3561s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1609
Product: mx-3561_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1610

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3570n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1611

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3570v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1612
Product: mx-3571s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1613

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-3571_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-3-100123/1614

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4050n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1615
Product: mx-4050v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1616

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4051_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1617

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4060n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1618
Product: mx-4060v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1619

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4061s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1620

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4061_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1621
Product: mx-4070n_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1622

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4070n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1623

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4070v_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1624
Product: mx-4070v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1625

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4071s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1626

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-4071_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-4-100123/1627
Product: mx-5050n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-5-100123/1628

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-5050v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-5-100123/1629

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-5051_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-5-100123/1630
Product: mx-5070n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-5-100123/1631

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-5070v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-5-100123/1632

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-5071s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-5-100123/1633
Product: mx-5071_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-5-100123/1634

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-6050n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-6-100123/1635

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-6050v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-6-100123/1636
Product: mx-6051_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-6-100123/1637

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-6070n_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-6-100123/1638

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-6070n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-6-100123/1639
Product: mx-6070v_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-6-100123/1640

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-6070v_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-6-100123/1641

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-6071s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-6-100123/1642
Product: mx-6071_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-6-100123/1643

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-6580n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-6-100123/1644

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-7081_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-7-100123/1645
Product: mx-7090n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-7-100123/1646

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-7580n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-7-100123/1647

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-8081_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-8-100123/1648
Product: mx-8090n_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-8-100123/1649

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b355wt_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1650

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b355wz_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1651
Product: mx-b355w_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1652

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b356wh_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1653

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b356w_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1654
Product: mx-b376wh_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1655

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b376w_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1656

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b455wt_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1657
Product: mx-b455wz_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1658

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b455w_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1659

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b456wh_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1660
Product: mx-b456w_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1661

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b476wh_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1662

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-b476w_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-B-100123/1663
Product: mx-c303wh_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-C-100123/1664

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-c303w_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-C-100123/1665

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-c303_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-C-100123/1666
Product: mx-c304wh_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-C-100123/1667

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-c304w_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-C-100123/1668

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-c304_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-C-100123/1669
Product: mx-m1056_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1670

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m1206_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1671

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m2630_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1672
Product: mx-m2630_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1673

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m2651_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1674

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3050_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1675
Product: mx-m3050_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1676

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3051_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1677

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3070_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1678
Product: mx-m3070_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1679

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3071s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1680

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3071_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1681
Product: mx-m3550_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1682

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3551_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1683

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3570_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1684
Product: mx-m3571s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1685

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m3571_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1686

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m4050_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1687
Product: mx-m4051_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1688

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m4070_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1689

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m4070_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1690
Product: mx-m4071s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1691

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m4071_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1692

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m5050_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1693
Product: mx-m5051_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1694

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m5070_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1695

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m5071s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1696
Product: mx-m5071_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1697

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m6050_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1698

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m6051_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1699
Product: mx-m6070_a_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1700

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m6070_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1701

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m6071s_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1702
Product: mx-m6071_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1703

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m6570_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1704

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Product: mx-m7570_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1705
Product: mx-m905_firmware					
Affected Version(s): -					
Improper Neutralization of Special Elements used in a	16-Dec-2022	7.2	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color	https://global.sharp/products/copier/info/info_security_2022-11.html	O-SHA-MX-M-100123/1706

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2022-45796**		
Vendor: sick					
Product: sim2000_firmware					
Affected Version(s): * Up to (excluding) 1.13.4					
Weak Password Recovery Mechanism for Forgotten Password	16-Dec-2022	9.8	Password recovery vulnerability in SICK SIM2000ST Partnumber 2086502 with firmware version <1.13.4 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the	https://sick.com/psirt	O-SIC-SIM2-100123/1707

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 1.13.4 as soon as possible (available in SICK Support Portal). **CVE ID : CVE-2022-47377**		
Vendor: Tenda					
Product: ac10_firmware					
Affected Version(s): 15.03.06.23					
Out-of-bounds Write	16-Dec-2022	7.5	Tenda AC15 V15.03.06.23 is vulnerable to Buffer Overflow via function formSetClientState. **CVE ID : CVE-2022-46109**	N/A	O-TEN-AC10-100123/1708
Product: f1203_firmware					
Affected Version(s): 2.0.1.6					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	20-Dec-2022	9.8	Tenda F1203 V2.0.1.6 was discovered to contain a command injection vulnerability via the mac parameter at /goform/WriteFacMac. **CVE ID : CVE-2022-46538**	N/A	O-TEN-F120-100123/1709
Buffer Copy without Checking Size of	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the mac parameter at	N/A	O-TEN-F120-100123/1710

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Input ('Classic Buffer Overflow')			/goform/GetParentControlInfo. **CVE ID : CVE-2022-46530**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the deviceId parameter at /goform/addWifiMacFilter. **CVE ID : CVE-2022-46531**	N/A	O-TEN-F120-100123/1711
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the deviceMac parameter at /goform/addWifiMacFilter. **CVE ID : CVE-2022-46532**	N/A	O-TEN-F120-100123/1712
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the limitSpeed parameter at /goform/SetClientState. **CVE ID : CVE-2022-46533**	N/A	O-TEN-F120-100123/1713
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the speed_dir parameter at /goform/SetSpeedWan. **CVE ID : CVE-2022-46534**	N/A	O-TEN-F120-100123/1714

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the deviceId parameter at /goform/SetClientState. **CVE ID : CVE-2022-46535**	N/A	O-TEN-F120-100123/1715
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the limitSpeedUp parameter at /goform/SetClientState. **CVE ID : CVE-2022-46536**	N/A	O-TEN-F120-100123/1716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the security parameter at /goform/WifiBasicSet. **CVE ID : CVE-2022-46537**	N/A	O-TEN-F120-100123/1717
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the security_5g parameter at /goform/WifiBasicSet. **CVE ID : CVE-2022-46539**	N/A	O-TEN-F120-100123/1718
Buffer Copy without Checking Size of Input	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the entrys parameter at /goform/addressNat.	N/A	O-TEN-F120-100123/1719

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			**CVE ID : CVE-2022-46540**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the ssid parameter at /goform/fast_setting_wifi_set. **CVE ID : CVE-2022-46541**	N/A	O-TEN-F120-100123/1720
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the page parameter at /goform/addressNat. **CVE ID : CVE-2022-46542**	N/A	O-TEN-F120-100123/1721
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the mitInterface parameter at /goform/addressNat. **CVE ID : CVE-2022-46543**	N/A	O-TEN-F120-100123/1722
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the cmdinput parameter at /goform/exeCommand. **CVE ID : CVE-2022-46544**	N/A	O-TEN-F120-100123/1723
Buffer Copy without	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer	N/A	O-TEN-F120-100123/1724

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			overflow via the page parameter at /goform/NatStaticSetting. **CVE ID : CVE-2022-46545**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the entrys parameter at /goform/RouteStatic. **CVE ID : CVE-2022-46546**	N/A	O-TEN-F120-100123/1725
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the page parameter at /goform/VirtualSer. **CVE ID : CVE-2022-46547**	N/A	O-TEN-F120-100123/1726
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the page parameter at /goform/DhcpListClient. **CVE ID : CVE-2022-46548**	N/A	O-TEN-F120-100123/1727
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the deviceId parameter at /goform/saveParentControlInfo.	N/A	O-TEN-F120-100123/1728

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46549		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the urls parameter at /goform/saveParentControlInfo. **CVE ID : CVE-2022-46550**	N/A	O-TEN-F120-100123/1729
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the time parameter at /goform/saveParentControlInfo. **CVE ID : CVE-2022-46551**	N/A	O-TEN-F120-100123/1730
Product: i22_firmware					
Affected Version(s): 1.0.0.3\\(4687\\)					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the funcpara1 parameter in the formSetCfm function. **CVE ID : CVE-2022-45665**	N/A	O-TEN-I22_-100123/1731
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Dec-2022	7.5	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the list parameter in the formwrlSSIDset function. **CVE ID : CVE-2022-45666**	N/A	O-TEN-I22_-100123/1732

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
Vendor: Tp-link					
Product: tl-wa7510n_v1_firmware					
Affected Version(s): * Up to (including) 3.12.6					
N/A	20-Dec-2022	7.5	An issue in the firmware update process of TP-Link TL-WA7510N v1 v3.12.6 and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46434**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1733
Product: tl-wa801nd_v1_firmware					
Affected Version(s): * Up to (including) 3.12.16					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-LINK TL-WA801N / TL-WA801ND V1 v3.12.16 and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46914**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1734
Product: tl-wa801n_firmware					
Affected Version(s): * Up to (including) 3.12.16					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-LINK TL-WA801N / TL-WA801ND V1 v3.12.16 and earlier allows attackers to execute arbitrary code or cause	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1735

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46914**		
Product: tl-wa901nd_v1_firmware					
Affected Version(s): * Up to (including) 3.11.2					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WA901ND V1 up to v3.11.2 and TL-WA901N V2 up to v3.12.16 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46910**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1736
Product: tl-wa901nd_v2_firmware					
Affected Version(s): * Up to (including) 3.12.16					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WA901ND V1 up to v3.11.2 and TL-WA901N V2 up to v3.12.16 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46910**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1737
Product: tl-wa901n_firmware					
Affected Version(s): * Up to (including) 3.11.2					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WA901ND V1 up to v3.11.2 and TL-WA901N V2 up to v3.12.16 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46910**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1738
Affected Version(s): From (including) 3.12.0 Up to (including) 3.12.16					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WA901ND V1 up to v3.11.2 and TL-WA901N V2 up to v3.12.16 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46910**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1739
Product: tl-wr1043nd_v1_firmware					
Affected Version(s): * Up to (including) 3.13.15					
Download of Code Without Integrity Check	20-Dec-2022	4.8	TP-Link TL-WR1043ND V1 3.13.15 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process.	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1740

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46428		
Product: tl-wr740n_v1_firmware					
Affected Version(s): * Up to (including) 3.12.4					
Download of Code Without Integrity Check	20-Dec-2022	4.8	TP-Link TL-WR740N V1 and V2 v3.12.4 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46430**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1741
Product: tl-wr740n_v2_firmware					
Affected Version(s): * Up to (including) 3.12.4					
Download of Code Without Integrity Check	20-Dec-2022	4.8	TP-Link TL-WR740N V1 and V2 v3.12.4 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46430**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1742
Product: tl-wr741nd_v1_firmware					
Affected Version(s): * Up to (including) 3.12.4					
Download of Code Without Integrity Check	20-Dec-2022	4.8	TP-Link TL-WR740N V1 and V2 v3.12.4 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1743

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46430**		
Product: tl-wr741nd_v2_firmware					
Affected Version(s): * Up to (including) 3.12.4					
Download of Code Without Integrity Check	20-Dec-2022	4.8	TP-Link TL-WR740N V1 and V2 v3.12.4 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process. **CVE ID : CVE-2022-46430**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1744
Product: tl-wr743nd_v1_firmware					
Affected Version(s): * Up to (including) 3.12.20					
N/A	20-Dec-2022	7.5	An exploitable firmware modification vulnerability was discovered on TP-Link TL-WR743ND V1. An attacker can conduct a MITM (Man-in-the-Middle) attack to modify the user-uploaded firmware image and bypass the CRC check, allowing attackers to execute arbitrary code or cause a Denial of Service (DoS). This affects v3.12.20 and earlier.	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1745

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2022-46432		
Product: tl-wr841nd_v7_firmware					
Affected Version(s): * Up to (including) 3.13.9					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WR841N / TL-WA841ND V7 3.13.9 and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46912**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1746
Product: tl-wr841n_firmware					
Affected Version(s): * Up to (including) 3.13.9					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WR841N / TL-WA841ND V7 3.13.9 and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46912**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1747
Product: tl-wr940n_v4_firmware					
Affected Version(s): * Up to (including) 3.16.9					
N/A	20-Dec-2022	6.5	TP-Link TL-WR940N V4 3.16.9 and earlier allows authenticated attackers to cause a Denial of Service (DoS) via uploading a crafted	N/A	O-TP--TL-W-100123/1748

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
			firmware image during the firmware update process. **CVE ID : CVE-2022-46139**		
Product: tl-wr941nd_v2_firmware					
Affected Version(s): * Up to (including) 3.13.9					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WR941ND V2/V3 up to 3.13.9 and TL-WR941ND V4 up to 3.12.8 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46435**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1749
Product: tl-wr941nd_v3_firmware					
Affected Version(s): * Up to (including) 3.13.9					
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WR941ND V2/V3 up to 3.13.9 and TL-WR941ND V4 up to 3.12.8 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46435**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1750
Product: tl-wr941nd_v4_firmware					
Affected Version(s): * Up to (including) 3.12.8					

Weakness	Publish Date	CVSSv3	Description & CVE ID	Patch	NCIIPC ID
N/A	20-Dec-2022	8.8	An issue in the firmware update process of TP-Link TL-WR941ND V2/V3 up to 3.13.9 and TL-WR941ND V4 up to 3.12.8 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image. **CVE ID : CVE-2022-46435**	https://www.tp-link.com/us/press/security-advisory/	O-TP--TL-W-100123/1751
Vendor: Zyxel					
Product: nbg7510_firmware					
Affected Version(s): * Up to (including) 1.00\\(abzy.2\\)c0					
N/A	21-Dec-2022	9.8	A DNS misconfiguration was found in Zyxel NBG7510 firmware versions prior to V1.00(ABZY.3)C0, which could allow an unauthenticated attacker to access the DNS server when the device is switched to the AP mode. **CVE ID : CVE-2022-38546**	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-dns-misconfiguration-in-nbg7510-home-router	O-ZYX-NBG7-100123/1752